Cloud Information Security: A Higher Education Perspective

Submitted in partial fulfilment
of the requirements of the degree of

Master of Science

of Rhodes University

Karl van der Schyff

Grahamstown, South Africa
February 27, 2014

Abstract

In recent years higher education institutions have come under increasing financial pressure. This has not only prompted universities to investigate more cost effective means of delivering course content and maintaining research output, but also to investigate the administrative functions that accompany them. As such, many South African universities have either adopted or are in the process of adopting some form of cloud computing given the recent drop in bandwidth costs. However, this adoption process has raised concerns about the security of cloud-based information and this has, in some cases, had a negative impact on the adoption process. In an effort to study these concerns many researchers have employed a positivist approach with little, if any, focus on the operational context of these universities. Moreover, there has been very little research, specifically within the South African context. This study addresses some of these concerns by investigating the threats and security incident response life cycle within a higher education cloud. This was done by initially conducting a small scale survey and a detailed thematic analysis of twelve interviews from three South African universities. The identified themes and their corresponding analyses and interpretation contribute on both a practical and theoretical level with the practical contributions relating to a set of security driven criteria for selecting cloud providers as well as recommendations for universities who have or are in the process of adopting cloud computing. Theoretically several conceptual frameworks are offered allowing the researcher to convey his understanding of how the aforementioned practical concepts relate to each other as well as the concepts that constitute the research questions of this study.

Contents

List of Figures

List of Tables

Acknowledgements

I would like to acknowledge the support I received from my supervisors as well as my family, especially Phyl Russell and my wife Lindsey.

Chapter 1

Introduction

1.1 Background Information

In recent years higher education institutions have come under increasing pressure to maintain high teaching standards. This has involved providing students with an environment that is conducive to research, whilst keeping within budgetary constraints [18]. Achieving this has presented university key stakeholders with many challenges, such as finding creative ways to teach relevant subject material in a cost effective manner using modern technologies.

With the promise of free applications such as Google Apps for Education[1] and Microsoft's Live@Edu[2], the adoption of cloud computing has become a viable option allowing universities to,

> *"...achieve large-scale efficiencies without sacrificing performance." [18, page 1]*

A reduction in the complexity of systems, cost savings from a supporting technologies perspective (e.g. less air-conditioning needed and a reduction in power requirements), a lighter administrative burden [88] and the ability to effectively deliver services to an increasingly mobile student population [6] offers the promise to alleviate the financial and operational pressures under which many South African universities find themselves. The University of California[3], for example, has adopted cloud computing enabling them to effectively meet research and conference deadlines, allocate resources efficiently whilst avoiding the costly pitfalls of over or under provisioning [88]. For Marist College[4] adopting the cloud has reduced costs by sharing a datacentre in Syracuse (New York) with

[1] http://www.google.com/enterprise/apps/education
[2] http://www.microsoft.com/liveatedu/free-email-accounts.aspx
[3] http://www.universityofcalifornia.edu
[4] http://www.marist.edu

other educational institutions [33]. Although Marist College opted to join what is commonly referred to as a community cloud, some universities, for example North Carolina State University (NCSU)[5] opted to keep their cloud solution in-house [33]. This has enabled NCSU to increase the productivity of students and information technology personnel alike, whilst reaping educational and technological cost savings.

However, Behrend *et al.* [6] warn that a successful cloud implementation depends on viewing several factors from both the student and the university's perspective. Of these factors information security is often cited as a key cloud adoption stumbling block [18, 88]. According to Tout, Sverdlik and Lawver [88] universities are particularly concerned with how the various university departments will integrate with the cloud security controls whilst maintaining confidentiality, integrity and availability of information.

The security concerns, of which some are listed above, have been explored by some authors, albeit in a positivist nature. Examples of these positivist studies can be found by looking at the work of the Data Security Council of India [25] who did a survey of Indian organizations and cloud providers in an effort to understand the developments in cloud computing. Although their survey revealed that 38% of surveyed organizations are using cloud computing, it fails to provide an in-depth understanding of why this is the case as well as the context in which these organizations operate.

Another study by Deloitte [27] examined similar cloud adoption aspects, but failed to take into consideration the various contexts of the organizations that were surveyed. The study conducted by Appirio [1] in 2010 resulted in a host of information, but relied solely on an online survey to gather information. In a study conducted by Ion *et al.* [47] a mixed approach was used where some in-depth interviews were conducted with participants in India and Switzerland. The results from the interviews were then contrasted with a survey that was conducted in the same countries. Although the study by Ion *et al.* [47] dealt with some aspects of cloud adoption in an in-depth manner, it was solely focused on the use of consumer cloud storage, which does not address the specific needs of universities.

Besides the information security concerns that have been investigated in the studies listed above, South African universities have to contend with additional challenges such as poor telecommunications infrastructure [41] and expensive Internet access [39].

To address these issues the then Department of Arts, Culture, Science and Technology started planning the South African National Research Network (SANReN)[6] in 2003, receiving final government approval for its implementation in 2006 (actual implementation taking place from 2011 onwards). The main thrust behind its construction was

[5] http://www.ncsu.edu

[6] http://www.sanren.ac.za

to enhance the environment in which research is conducted at South African universities, allowing them to participate in global research [74]. The implementation of this project was entrusted to the Council for Scientific and Industrial Research (CSIR) Meraka Institute[7] who has been assisted by The Tertiary Education and Research Network of South Africa (TENET)[8] in the running of SANReN (SANReN roll-out status available on this site[9]). In addition to SANReN connectivity South African universities do not all serve the same purpose. To differentiate South African universities according to their intended purpose the Centre for Higher Education Transformation (CHET)[10] issued a report where South African universities are grouped into three distinct clusters. To construct these clusters the following data sources were used [14]:

- Higher Education Information Management System (HEMIS) data on staff and students,
- Data on research publications, and
- Financial statements of higher education institutions.

The groups were colour coded by CHET according to their purpose, which are stated as follows:

- **Red Cluster**: Five research-intensive universities are found within this cluster. They produce the majority of South African postgraduates and academics. These universities exhibit high rates of success, a large proportion of PhD qualified lecturers, higher levels of income and research output whilst maintaining a low level of student vs. staff ratio [57].
- **Green Cluster**: The nine universities within this cluster display levels of performance which declined after merging with *"historically disadvantaged"* tertiary institutions [57].
- **Blue Cluster**: The remainder of South African universities fall within this cluster and have relatively low levels of performance in terms of postgraduate success, qualified staff, income and research outputs. However, these universities do exhibit high levels of enrolment in science, technology and engineering with a high student vs. staff ratio [57]. Moreover, the CHET report [14] also emphasises that these universities provide *"occupation ready"* education to a relatively poor student population.

Keeping the above facts in mind it becomes clear that a study focused on such a diverse group of South African universities will offer valuable information since their operational and security contexts will almost certainly differ. Armed with this information university key stakeholders will be able to not only make informed decisions around the adoption of cloud computing, but also the information security concerns that could influence its adoption.

[7] http://www.csir.co.za/meraka

[8] http://www.tenet.ac.za

[9] http://www.sanren.ac.za/status

[10] http://www.chet.org.za

1.2 Problem Statement

Security concerns remain a key issue in the adoption of cloud computing in South African universities. This is confirmed by Monfared [60] who states that concerns with regard to the confidentiality, integrity and availability of information have been the main driving force behind the slow cloud adoption rates. Moreover, the views of users surrounding cloud security have been captured mostly through the use of surveys and positivist approaches. In addition to this, most studies lack context and do not provide much in-depth detail. With the expectation that universities utilize cutting edge technology and pursue leadership in ICT adoption whilst creating awareness, it makes sense to understand what the views of key stakeholders are with regard to cloud information security.

The reality is that very little research is available on the topic from a South African perspective. The unique operational requirements, the effects of SANReN, and the different contexts within which universities operate may result in unique cloud computing requirements. There is therefore a need to conduct an in-depth investigation into the information security concerns surrounding cloud computing from the perspective of key stakeholders at South African universities.

To address the various information security concerns highlighted in the problem statement an answer to the following main research question needs to be found:

> ***What are the views of key stakeholders within South African universities with regard to the security of cloud-based information?***

Answering this question could assist South African universities in the cloud adoption process by highlighting specific security concerns. It is unlikely that each individual university will be able to enumerate all these security concerns, which is where such a diverse collection of views on cloud information security would be useful. This information could also be used by cloud providers, which could assist them in the creation of cloud services tailored to the specific needs of South African universities.

To address the various facets of the main research question the following two sub-questions need to be investigated:

1. ***What are the views of key stakeholders within South African universities on how cloud computing threats affect the security of cloud-based information?*** The purpose of this question is to investigate the views of key stakeholders with regard to the effects cloud-based threats have on the security of cloud-based information. Data gathered here will enhance the knowledge key

stakeholders have with regard to cloud computing threats and the effect these threats have on how South African universities evaluate whether or not to adopt the cloud.

2. ***What are the views of key stakeholders within South African universities with regard to the security incident response life cycle in a higher education cloud?*** The purpose of this question is to understand how South African universities view the security incident response life cycle and whether it is an adequate means of responding to security incidents in the cloud. This understanding could guide other South African universities who are either in the process of adopting or evaluating the cloud.

1.3 Terms and Definitions

To assist the reader in understanding this research the following important terms and definitions are provided and are subsequently applicable throughout this study.

Cloud Computing: Although this study discusses various cloud deployment models the emphasis of this study is to investigate cloud computing within a third party cloud (i.e., services hosted by a cloud provider).

Cloud Provider: An organization which provides cloud services to cloud subscribers for example South African universities. This could be on an enterprise or consumer level and may or may not be a charged-for service. Examples include Salesforce[11] which is a paid for cloud service and Google Apps for Education which is not.

Cloud Subscriber: Any organization which makes use of or subscribes to cloud services that are being offered by a cloud provider.

In addition to these definitions the reader will also be directed to specific websites (found in the footnotes) containing additional information on the topics explored by this study.

1.4 Aims of the Research

The primary objective of this study is to gain an in-depth understanding of how the information security concerns pertaining to the adoption of cloud computing affect the views of key stakeholders within South African universities with specific reference to cloud information security. The study also aims to investigate the levels of awareness with regard to cloud security threats and the extent to which university key stakeholders view these as

[11] http://www.salesforce.com

cloud adoption stumbling blocks. Thirdly, it aims to evaluate security incident response within higher education clouds by investigating the views of university key stakeholders with regard to the security incident response life cycle.

1.5 Contribution

Several calls for further research into cloud computing have been made. These calls for further research pertain specifically to the verification of integrity, incident handling and data confidentiality [34]. Pardeep [55] states that there is a need to understand why consumers (university key stakeholders) do not fully trust cloud computing from a business and technological perspective. Both of these issues are addressed by this research. The United States National Institute for Standards and Technology (NIST)[12] states that an understanding of the operational context an organization finds itself in is needed before one can determine the suitability of cloud services [64]. Khorshed, Ali and Wasimi [50] also state that,

> *"... it is the perception of the customers which dictates whether they or their organizations are willing to join cloud computing that matters." [50, page 835]*

A study on the information security concerns of cloud computing will be beneficial to the cloud community at large and specifically to South African universities. Having a clear understanding of the views of key stakeholders with regard to cloud computing threats, incident response and the underlying concerns surrounding the confidentiality, integrity and availability of information holds the promise of understanding cloud adoption at universities. This is not only limited to institutions of higher education, but may be universally applicable. Cloud adopters and providers could use this information as part of a larger security driven adoption framework. Also, because these views are presented and shaped by the context in which the participants operate it becomes a vital part of the planning and preparation phases of a cloud adoption strategy, especially within universities that may have similar contextual characteristics.

1.6 Methodological Approach

It is important to note the author's orientation to knowledge. This research will be performed within an interpretivist framework. As Lin [56] suggests, interpretivism illustrates what an identified general pattern looks like in

[12] http://www.nist.gov

practice as well as understanding it. Conversely a positivist approach would only identify these general patterns. Another important aspect of the chosen approach is highlighted where Lin [56] states that in an interpretive study constructs are part of the context it studies and thus less likely to be adversely affected by inaccurate generalizations. In addition to the previous statement, Walsham [90] captures why an interpretivist approach will allow this study to gain the insights it sets out to identify by arguing that interpretivism allows the researcher to increase his understanding of the phenomena within a specified context and cultural setting whilst allowing for the investigation of the phenomena from the participants perspective. Additionally Kroeze [54] states that the acquisition of meaning and understanding is the primary purpose of interpretivist research. Below some of the core interpretive concepts of this study are briefly discussed (a more detailed discussion can be found in *Chapter Three*).

1.6.1 Philosophical Assumptions

During this study the researcher has made the following philosophical assumptions. Together they form the intellectual framework upon which the research is based.

- **Ontological Assumptions**: From the participants point of view, reality (ontology) is socially and experientially constructed [89]. Furthering this, it is believed that an in-depth understanding with regard to the construction of meaning can be obtained by investigating the qualitative data gathered [89]. The researcher will not be able to distance himself from the socially constructed reality and an emphasis will be placed on the context within which the research takes place [54]. Taking note of the context, the experiential background of the participant and the exhibited phenomena (in this case participant views) will allow the researcher to acquire the required knowledge (i.e., understanding with regard to participant views).
- **Epistemological Assumptions**: During this study the researcher and the research participants are to be regarded as an entwined entity. This will affect the interview results, since the actual interview process is influenced by the interaction that occurs during each interview [89]. Subjectivity, from the researcher's point of view, is assumed and accepted. Accurate information is available and needs to be uncovered during the interview process, making knowledge achievable in this manner [52].

1.6.2 Research Method

Approaching this study from a qualitative perspective will afford the researcher the opportunity to study the participants in their operational context, whilst at the same time attempting to interpret the views of the participants and their associated meanings [46].

1.6.3 Data Collection

The proposed data gathering process will involve a two phase approach, with the first phase of data being collected via an online survey. The primary purpose of the survey will be to get an overarching view of what university key stakeholders know about the cloud, specifically with regard to cloud computing threats, security incident response and the information security concerns pertaining to its adoption. It is anticipated that the results of this survey will assist the researcher in the construction of a relevant interview guide with which to collect primary data.

The second phase of the data collection process will involve conducting in-depth interviews with key stakeholders (from South African universities). This qualitative approach has been selected specifically because it allows the researcher to get closer to the participant's views [46]. Both the online survey and the in-depth interviews will be piloted to ensure that the interview questions are capable of soliciting relevant information.

1.6.4 Data to be collected

This study intends collecting data on not only how key stakeholders view cloud information security concerns, but also how their operational context influence their views. For these reasons the online survey will be collecting data directly related to the conceptual framework illustrated in *Section 2.9*. Together with the research questions (see *Section 1.2*) it is believed that this conceptual framework will allow for the initial collection of data (via online survey), which could then be used in the creation of the primary data collection instrument (the interview guide).

1.6.5 Sources of Data

The participants (key stakeholders) of this study will include IT Managers, Technical Managers, Operations Managers, IT Directors, Systems Managers and System Administrators from South African universities. This specific group of key stakeholders has been selected because successful cloud implementations depend on the beliefs of these key stakeholders [6]. Regardless of their technical proficiency, their views will be valuable to cloud providers and other universities with similar contextual backgrounds, since this study aims to focus more on interpreting the relationship between the participant's views (on cloud information security) and their operational context. Additionally, qualitative studies often require diversity and as such researchers should find participants who,

> *"... represent a variety of positions in relation to the research topic" [52, page 29]*

This is reflected in the variety of job roles interview participants operate in.

1.6.6 Data Analysis

Because the researcher expects certain themes to emerge as the transcribed interview data is processed [38], thematic analysis has been chosen as the primary method of data analysis. This process is to be more theory driven and will be based largely on the concepts discussed in the literature review. The researcher will be making use of a specific approached, as outlined by Braun and Clarke [10] (see *Section 3.8* for more detail). As such, it is anticipated that the initial conceptual framework will change throughout the analysis process.

1.6.7 Limitations & Bias

Although much of the literature is focused on commercial organizations the data collected will focus exclusively on South African universities. Also, the views being investigated will be limited to key stakeholders working within the IT departments of the participating universities. It is worth noting that the focus of the literature review and the subsequent investigations will not be vendor specific although some examples may be mentioned. Influences, like those introduced by SANReN, also limits the applicability to universities outside the South African context, but given the development of similar research networks in Africa is still relevant.

The method of analysis (thematic analysis) relies heavily on recurring themes, which necessitates clearly stating what constitutes a theme. This study is thus limited by the mechanisms that were used during the identification of the said themes. The fact that thematic analysis makes extensive use of quotes (to support certain arguments), adds to its reliance on the accuracy of transcriptions.

The interpretations of data are influenced by the researcher's background and context. In interpretivist studies results cannot necessarily be generalized to other situations and thus only within the context of each participating university [53]. This research will also be limited by the subjective nature that characterizes interpretative research. Interpretivism is further limited in the sense that it describes the status quo and does not recognize the effects that political and ideological factors have on knowledge and social reality [58].

1.6.8 Assumptions

Participating key stakeholders are assumed to be knowledgeable enough about the cloud, enabling them to have substantive views on the security of cloud-based information.

1.7 Dissertation Structure

The remainder of the dissertation is structured as follows:

- **Chapter Two:** Provides a review of the literature relevant to the research that is to be undertaken. The discussions within the literature review start off with a broad overview of cloud computing followed by discussions relevant to the research questions. The literature review concludes by presenting the reader with a conceptual framework which will guide the initial data collection process (the online survey).
- **Chapter Three:** This chapter addresses the methodological approach of this study and contains detailed discussions on the involved processes. It concludes with the formulation of a set of survey and interview questions together with their purpose as well as a detailed discussion on thematic analysis.
- **Chapter Four:** This chapter starts by presenting the results of the online survey. This takes the form of several graphs and will be accompanied by a brief interpretation of these graphs. Following this the researcher will discuss the results of the in-depth interviews paying particular attention to the process of analysis, which culminates in the creation of a thematic map. In addition to the thematic map the researcher will also illustrate two conceptual frameworks aligned with each main theme. The chapter concludes with the researcher using the thematic map and conceptual frameworks in the construction of a cross-case narrative.
- **Chapter Five:** Within this chapter the reader will be presented with the findings of this study, explanations of how the research questions were addressed as well as how the execution of the latter two processes contributed to the field of cloud computing. This chapter provides South African universities with some recommendations and identify areas of future research. The chapter concludes by discussing the limitations of this study as well as providing the reader with a brief summary of the dissertation.

Chapter 2

Literature Review

2.1 Introduction to the Cloud

In *Section 2.2* of this chapter the reader will be presented with the various architectural components of cloud computing, followed by a discussion surrounding the technologies that *"enable"* cloud computing (see *Section 2.3*). An in-depth discussion of cloud computing threats and their effect on the confidentiality, integrity and availability of cloud-based services and data will follow in *Section 2.5*. After a discussion regarding the means to address these cloud computing threats (*Section 2.6*) and security concerns, a review of the literature about the security incident response life cycle and how it relates to cloud computing will follow (see *Section 2.7*). This chapter concludes with a discussion centred around recent surveys that have been conducted with regard to the adoption and use of cloud computing.

Cloud computing is not a new concept and shares many similarities with the time sharing systems of the 1960's as well as the grid/network computing systems prevalent during the 1990's [51]. It offers users and organizations a convenient way of computing without having to understand the intricacies of exactly how processing is performed in the cloud [66]. This in turn forces users and organizations to trust the cloud provider, which raises issues about the security and reliability of the cloud [66]. Chen and Sion [15] suggest that these security concerns are the main reasons why organizations are hesitant to adopt cloud computing. The Data Security Council of India provides evidence to support this claim. In their survey (conducted in 2010) 95% of the participating organizations agreed that data security and privacy are the biggest hurdles when considering a move towards the cloud [25]. Confidentiality, legal and contractual concerns are also mentioned by Joint, Baker and Eccles [49].

Similarly Farrell [37] states that even with all the information security benefits, cloud adoption is still impeded by the perceived information security risks and legal challenges faced by most organizations. Additionally, during a survey conducted (2010) by PriceWaterhouseCoopers (PWC) 23% of the participants stated that the greatest risk to their current cloud strategy is the inability to control how security policies are implemented at the cloud provider [69].

Notwithstanding all the information security concerns, many organizations are actively adopting cloud computing. Appirio [1], who conducted an online survey in 2010, found that 38% of the 155 respondents singled out IT leadership as the main driving force behind the misconceptions surrounding cloud computing. It is for these reasons that early adopters are mostly hosting less sensitive data with cloud providers [47] and in most cases opt for a hybrid cloud [25].

It is also worth noting these surveys followed a positivist approach lacking any in-depth approaches.

2.2 Cloud Architecture

In order to put the views of the key stakeholders into perspective one needs to have an understanding of cloud computing architecture as well as what defines cloud computing. The National Institute for Standards and Technology (NIST)[1] provides the following definition of cloud computing:

> *"Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction" [64, page vi]*

Cloud computing architecture is based on the cloud deployment and delivery models, which forms a foundation upon which the various cloud services are built. These are illustrated in *Figure 2.1*.

2.2.1 Cloud Deployment Models

In essence the various deployment models indicate where the cloud services offered in the second layer of *Figure 2.1* will be located physically, who owns the infrastructure and who controls the infrastructure [64]. Cloud deployment models can be defined as:

[1] http://www.nist.gov

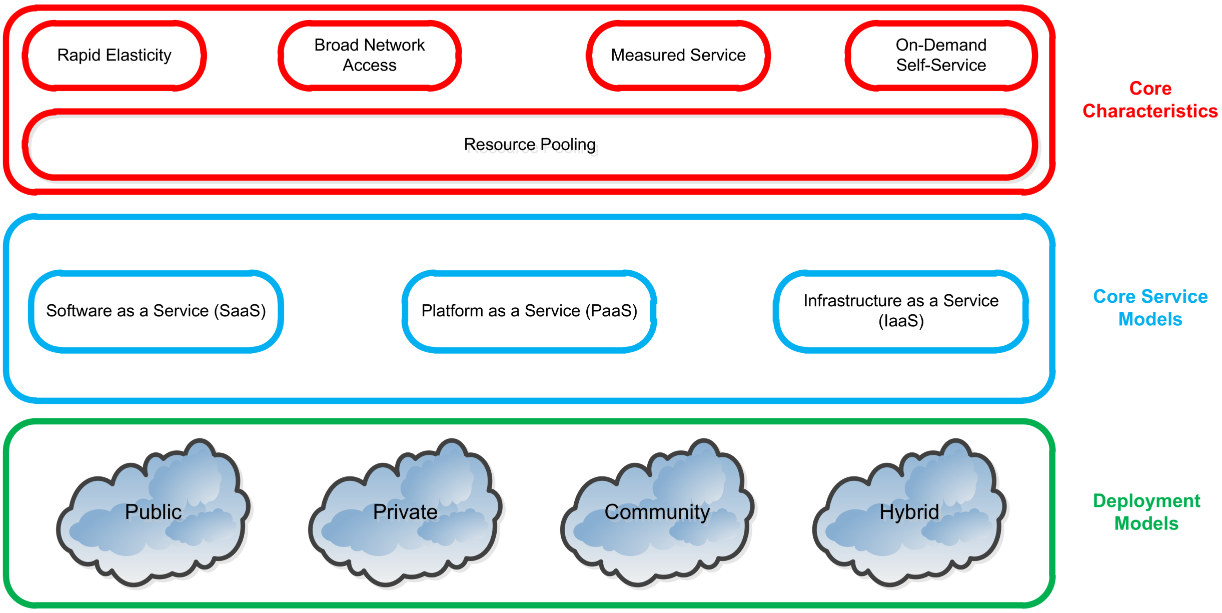


Figure 2.1: Cloud architecture (adapted from NIST [64])

> *"Deployment models broadly characterize the management and disposition of computational resources for delivery of services to consumers, as well as the differentiation between classes of consumers." [64, page 3]*

The four cloud deployment models are:

- **Public Cloud Computing**: This is a deployment model where the infrastructure and services are made available to the general public and is operated by a cloud provider [98]. Here the interfaces to interact with the cloud are provided by web browsers [71]. This model is based on the principle whereby payment for usage only is procured, which makes it cost effective. Ramgovind *et al.* [71] furthers their discussion of deployment models by stating that it is the most insecure of all the cloud computing service models and relies on the security of the offered applications and services. It is suggested by Ramgovind *et al.* [71] that responsibilities should be negotiated with the cloud provider in the Service Level Agreement (SLA) to ensure that the proper security management structures are put in place. Gmail[2] is just one example of such a public cloud.

- **Private Cloud Computing**: With private cloud computing, the cloud infrastructure is owned by the organization and full control can be exercised over its operation [30]. According to Dillon, Wu and Chang [30] reasons for using a private cloud include:

[2] http://www.gmail.com

  - Optimal use of the local computing infrastructure,
  - Security is more manageable,
  - Costs to migrate data to the public cloud are still prohibitive (typically bandwidth),
  - Allows for complete control over critical services, and
  - Often is used by academics as a means of conducting research.

  Private clouds may vary in size and are usually based on either Microsoft Hyper-V[3] or VMware vSphere[4].

- **Community Cloud Computing**: Here the computational resources are shared between two or more organizations that have the same security and/or compliance requirements [37, 98]. Dillon *et al.* [30] states that although a community cloud would normally be hosted by a third party cloud provider, it may also be hosted by one of the members of the community cloud. An example of a community cloud could be any system whose access is shared amongst the members of that community cloud. These could take the form of library management systems or municipal databases etc.

- **Hybrid Cloud Computing**: Some components are outsourced to a cloud provider and some parts of the cloud infrastructure are kept in-house. It is stated by Ramgovind *et al.* [71] that it has an open architecture, which ensures interfacing with other management controls. Any of the examples listed above can form the building blocks of a hybrid cloud as long as the cloud components are used in a public/private combination.

Although not traditionally included as a deployment model in the literature, Amazon has recently introduced another deployment model, the Virtual Private Cloud (VPC) [30]. This model combines the best features of the public and private deployment models whilst still allowing the client to only pay for their usage [30].

2.2.2 Cloud Delivery Models

In *Figure 2.1* the three cloud delivery models are depicted on the level immediately above the cloud deployment models. The Cloud Security Alliance [19] states that Infrastructure-as-a-Service (IaaS) forms the basis onto which Platform-as-a-Service (PaaS) is built, which in turn forms a foundation for Software-as-a-Service (SaaS). This is an important aspect of which to take notice, since the cloud delivery models inherit information security concerns from one another [19]. As far as overall control goes, an organization that subscribes to an IaaS offering can expect to have more control than with a PaaS or SaaS offering, with SaaS providing the lowest level of control [27]. As far

[3] http://www.microsoft.com/en-us/server-cloud/hyper-v-server/default.aspx

[4] http://www.vmware.com/products/datacenter-virtualization/vsphere/overview.html

as the responsibilities are concerned Subashini and Kavitha [84] state that both the provider and the customer's responsibilities vary greatly depending on the cloud delivery model in use. This makes understanding the various cloud delivery models important from an architectural point of view.

The various cloud delivery models are:

- **IaaS (Infrastructure-as-a-Service)**: A client is able to rent a virtual machine image as a service [73] or even rent a collection of virtualized servers organized into a virtual private data centre [31]. It also affords the client the most control in terms of what operating system and applications can be loaded [98]. However, the client does not have control over the actual cloud infrastructure. Amazon's IaaS offering, namely EC2[5], is one example.
- **PaaS (Platform-as-a-Service)**: According to Ramgovind *et al.* [71] the tools made available to PaaS clients allows for rapid application development in a homogeneous web environment. It grants the client less control than IaaS, but still more flexibility than that which is offered by SaaS. Added functionality may come at the cost of vendor lock-in, but this can be offset against the savings in operational expenses [71]. Examples include Microsoft's Azure[6] development platform and Google's AppEngine[7].
- **SaaS (Software-as-a-Service)**: Here applications and services, like webmail and remote backup, are hosted with the cloud provider and made available to the customer over the Internet, usually via a web browser [44, 84]. Dahbur *et al.* [24] states that in this model the user exchanges the capital expenses of software (e.g., licenses) for operational expenses. Because applications are delivered over a web browser, organizations have to take extra precautions with regard to their client side security, since this can become a point of vulnerability even if the cloud infrastructure is secure [71]. Insider breaches, application vulnerabilities and general availability concerns are real and often dissuade most organizations from adopting SaaS outright [35]. Popular examples of SaaS cloud offerings are Google Apps[8], Dropbox[9] and NetSuite[10].

Dillon *et al.* [30] includes Data-storage-as-a-Service (DaaS) in their list of delivery models. The authors state that with this delivery model, cloud storage is provided to the clients as needed. They do however admit, that it can strictly be defined as a type of IaaS. Their motivation for defining it as a separate delivery model is twofold. Firstly it allows for the client to only pay for the storage they actually need and secondly it allows the client to effectively work with very large datasets. An example of a DaaS provider is Amazon with their S3[11] cloud storage

[5] http://aws.amazon.com/ec2
[6] http://www.windowsazure.com/en-us
[7] http://code.google.com/appengine
[8] http://www.google.com/apps/intl/en/business
[9] https://www.dropbox.com
[10] http://www.netsuite.com/portal/home.shtml
[11] http://aws.amazon.com/s3

offering. The researcher would like to point out that although there are other service models the aforementioned types form the core of what is considered a cloud service model.

The discussion above shows that knowledge, with regard to cloud architecture, is useful especially during the planning and preparation phases of cloud adoption. Cloud computing, and indirectly the various cloud delivery models, do however, depend on a number of technologies that enable it to deliver the services as described above. It is these technologies that are discussed in the next section.

2.3 Cloud Enabling Technologies

As with most technical solutions and products, cloud computing is also based on other technologies. These technologies are commonly referred to as enabling technologies and are briefly discussed below:

- **Virtualization**: Virtualization is increasingly being used by cloud providers for IaaS, PaaS and SaaS offerings. According to the Cloud Security Alliance [19] it has enabled cloud computing to exhibit many of its current advantages (i.e., multi-tenancy and data centre reduction). Essentially it has made public cloud computing affordable and is also its biggest enabling technology. In [73] it is even claimed to be the central technological feature that makes cloud computing possible. Similarly Zissis and Lekkas [98] state that virtualization is what separates grid computing from cloud computing. Dahbur, Mohammed and Tarakji [24] state that virtualization is the most influential concept in cloud computing. Virtualization can be summed up as follows:

  > *"Cloud Computing employs the virtualization technology to offer a secure, scalable, shared and manageable environment" [26, page 1]*

  Virtualization, at its core, is a technology that enables a cloud provider to run multiple sessions or instances of different operating systems and the applications that accompany them. These instances are called virtual machines and act in exactly the same way as their physical counterparts. By using hardware in this way one quickly realizes why cloud computing is so cost effective. According to Dahbur *et al.* [24] virtualization allows the hardware to present itself in different capabilities, which is central to the concept of cloud computing. The authors also explain how it is possible for services to be rapidly deployed and the flexibility of those deployed services. In 2010 a survey conducted by PriceWaterhouseCoopers (PWC) [69] found that although virtualization has enabled organizations to embrace cloud computing, there are still some (10%) organizations who claim that it introduces more security risks. Companies like, VMware[12] and Microsoft[13] are often listed as providers of virtualization technologies.

- **Web 2.0**: Since most of services that the public cloud delivers to the client are web-based this should come as no surprise. According to Wang *et al.* [92] Web 2.0 is a technology that aims to enhance the creativity and functionality of the web by utilizing the following technologies:
  - Cascading Style Sheets,
  - Semantic Web Technologies,
  - Privacy management tools, and
  - Technologies that enhance the look and feel of the web interfaces, like AJAX and XHTML.

  Because cloud computing leverages the web to deliver dynamic content, it would make sense to use these Web 2.0 based technologies when delivering cloud services [92].

- **High Speed Internet**: Robust and reliable network connectivity has made cloud computing a reality. Even more so in first world nations, as in the United States and Europe. Unfortunately the same cannot be said of developing countries, where reliable network communications is not commonplace. In South Africa specifically the slow introduction of fixed line broadband services has had a negative impact on the growth of the Internet in South Africa [40].

2.4 Why adopt the Cloud?

The Ponemon Institute found that 67% of organizations in the United States and 62% of European organizations are already using SaaS services [68]. Similarly a study, conducted by Appirio [1], 68% of public cloud adopters indicated that most of their applications will be in the public cloud in the next 3 years. There are a number of reasons why organizations would want to adopt the cloud.

The cloud enhances computing flexibility, since users are able to combine disparate technologies into usable services [65, 98]. Similarly the authors of [24] also state that cloud computing allows for the ability to locate resources and release them as needed. This creates flexibility, elasticity and responsiveness.

Better security and reliability can also be obtained. This is contradicted by Armbrust *et al.* [2] where the authors claim that data confidentiality is one of three obstacles that affect cloud adoption. On the other hand Zizzis and Lekkas [98] argue that automation and focused security resources also result in enhanced security capabilities.

[12] http://www.vmware.com

[13] http://www.microsoft.com

Organizations could benefit from the economic advantages the cloud offers [9,49,55,98]. These cost savings are made possible by increasing server utilization, using less data centre floor space and consuming less power. Cloud computing could alleviate the need for costly resources in the case of start-ups [44]. Ultimately because the cloud model is typically priced in terms of the amount of storage space used and processing cycles expended, one would be able to equate it with everyday commodities (i.e., electricity, oil and natural gas [23,48]), hence the name *"utility computing"* as used by Jaeger, Lin and Grimes [48]. In fact the concept of *"utility computing"* has been predicted as early as 1969 by Leonard Kleinrock who worked for ARPANET at the time [12].

The cost savings introduced by cloud computing are even more pronounced in situations where providers make use of multi-tenancy. Its use does, however, lead to concerns about the confidentiality of cloud-based information. This sentiment is not shared by all researchers. Durkee [31] states that the commoditization of cloud computing could actually make vendors move away from enterprise requirements, which initially brought it into the limelight.

Since organizations' data can now be hosted off-site within a cloud, cloud computing enables organizations to gain access to disaster recovery solutions at a much lower price [23]. Hosting sensitive data off-site within a cloud will save money and enhance the availability of the information since it is accessible from multiple locations [98].

Cloud providers employ and have access to individuals who are experts in the field of cloud computing. These individuals are indirectly available to the cloud subscriber, which in turn affords subscribers the opportunity to use their own staff members more effectively [64]. Cloud subscriber are then allowed to regulate and control the resources they consume without intervention from the cloud provider [24].

Cloud computing can thus be seen as an attractive alternative to the traditional in-house datacentre. However, this does not mean the idea of a traditional data centre is dead. In fact the Ponemon Institute [68] state that only 16% of European and 22% of United States organizations are currently hosting business critical applications in the public cloud.

2.5 Threats in the Cloud

The security required by networks and datacentres is not easy to implement. This is made even more difficult by the shared nature (multi tenancy) of cloud computing [50]. Thus making a choice as to which security mechanisms are sufficient requires sound judgement with regard to the threats that can be expected [50].

From an information security perspective threats represent the potential that a system may be exploited with negative consequences to its operation [76]. It is often confused with the concept of vulnerability, risk or exposure [24]. To put the concept of a threat into perspective Saripalli and Walters [76] state that an attack is the actual exploitation of a vulnerability, which leads to the threat being realised.

There are a host of serious threats to an organization's information [30] and thus apprehension towards cloud adoption [50] because of these threats. It therefore becomes essential to understand what threats to expect when adopting the cloud. Accordingly the Cloud Security Alliance [20] proposes that cloud computing infrastructures are typically exposed to the following threats:

Insecure Application Programming Interfaces (API's). Cloud providers expose certain programming API's to their clients that can be used to interact and effectively manage their cloud environments (e.g., monitoring and provisioning). Wrenn [94] elaborates by stating that attacks which bypass authentication may result in the unauthorized use of administrative functions. The use of *"cloud brokers"* worsens the situation by introducing additional API's to exploit as well as additional layers of abstraction. Many of these vulnerabilities are shared amongst the API's and the web application layer, which poses an additional problem, since cloud services are commonly accessed via web browsers (which operate within the web application layer) [50]. Although the Cloud Security Alliance proposes the use of some mitigation techniques Khorshed *et al.* [50] states that some flaws still exist. Two flaws being the inability to effectively audit the usage of API's and that current logs are unusable in the reconstruction of any managerial actions that have been taken. This in turn negatively impacts on the confidentiality, integrity and availability of the information stored in the cloud [94].

Account or service hijacking. The Cloud Security Alliance [20] suggests that organizations should familiarize themselves with the means to defend against these threats. By means of stealing credentials criminals gain unauthorized access to the cloud infrastructure, often using it as a base of operations. The access they are granted by obtaining the stolen credentials compromises the confidentiality, integrity and availability of the cloud services and data [82]. Wrenn [94] agrees, but adds that account hijacking is a *"constant threat"* often perpetrated under the guise of the victim's (organization) identity. Khorshed *et al.* [50] states that not only do stolen credentials allow an attacker to gain access to confidential information, but could also assist in eavesdropping on the actions of the client, which according to Shin and Kobara [82] are exacerbated in a single sign-on environment.

Malicious Insiders. Many organizations are faced with the activities of malicious insiders who have the ability to negatively impact critical components of an organization [20]. According to the Cloud Security Alliance, as the popularity of the cloud and the involvement of humans increases, it will become vital for clients to know exactly how cloud providers intend to deal with malicious insiders. Wrenn [94] states that cloud providers lack transparency, as far as employment practices go, as well as not being able to effectively monitor administrative employees. This in turn leads to the compromise of the client's cloud-based data.

Data Loss or Leakage. Data loss or leakage has the potential to negatively impact the levels of trust, corporate image and could result in financial loss [20]. The dynamic nature of the cloud magnifies this impact even more, across all cloud delivery models. Such negative incidents are illustrated by Dahbur *et al.* [24] where the authors mention specific incidents of data loss in the cloud. Wrenn [94] states that data loss might occur due to storage hardware failure as well as inadequate backup procedures. This can be associated with poor management practices on the part of the cloud provider. With data loss or leakage not being limited to only specific cloud delivery models, it thus becomes essential to understand how poor infrastructure management and hardware failures can affect the confidentiality of cloud-based data.

Abuse of Cloud Computing. The anonymity, ease of registration and weak fraud detection mechanisms on the part of the cloud provider, has enabled many cyber criminals to execute their criminal activities with little judicial recourse [20]. It's also possible for cloud subscribers to host malicious (e.g., phishing) websites, which exposes the cloud provider and end-user to cloud threats [60]. Monfared [60] states that the abuse is not only limited to clients, but also to end-users who could store data of an illegal nature in the cloud. However, according to Khorshed *et al.* [50] monitoring and analysis of network traffic, as suggested by the Cloud Security Alliance, is currently constricted by privacy laws. This complicates matters for cloud providers who are not able to effectively identify cloud abuse. Cloud computing abuse thus has the potential to expose clients, cloud providers and end-users to the compromise of the confidentiality and integrity of their cloud-based data.

Unknown Risk Profile. The Cloud Security Alliance states that even though a newly adopted cloud infrastructure may exhibit various functions, it does not address the concerns relating to how the cloud provider manages internal processes and procedures (e.g., auditing, software updates and logs). The client is also not always aware of what information will be disclosed post security incident [20]. According to Wrenn [94] these concealed cloud processes and procedures are important and often ignored by the clients. This leads to serious concerns with regard to the safety of the client's information. Chow *et al.* [17] expands on the discussion above by including the cloud specific threats listed below:

- **Greater Network Attack Surface**: The users of third party cloud services need to protect the mechanism that is used to interact with the cloud, which is often outside the organizational firewall.

- **Single Point of Failure**: Although the cloud provides enhanced availability, it is offset by the fact that it exhibits more single points of failure (centralized server farms and communication infrastructures) which attackers may use to cripple access to cloud-based services.
- **Authorization of Data Mash-up**: As the popularity of cloud computing increases, it is likely that organizations may encounter an increasing number of services that perform data mash-ups. This may result in data leaks as well as security issues surrounding authorized access to the various sets of data used in the mash-ups.

In addition to the above Dawoud, Takouna and Meinel [26] list the following cloud specific components together with their associated threats:

Utility Computing. Here the attackers to the cloud infrastructure gain access to services for which they have not paid. It is mainly the cloud providers' responsibility to ensure that this does not take place.

Cloud Computing Software. Both open source and commercial software utilize web service protocols, like the Simple Object Access Protocol (SOAP)[14]. Even when using web services security, to ensure proper encryption of the SOAP header, there are still known attacks for these web service protocols. In one such attack, the *"wrapper attack"*, an attacker essentially creates a duplicate of an Extensible Markup Language (XML) signature that contains additional malicious instructions [73]. The major delivery platform of SaaS services and applications is the average web browser. As such, its security can also be seen as a threat, since browsers in general do not take advantage of the XML signatures. This makes them rely on Transaction Layer Security (TLS). TLS on the other hand requires digital certificates to be installed on the web pages, which not all of them have [73]. So even the exploitation of browsers is a threat. With web services forming such an integral part of cloud software, ignoring its associated threats is not recommended, since its security underpins the security of the cloud service as a whole.

Computing Hardware. In a recent study by Halderman *et al.* [43] the authors demonstrate how a phenomenon called *"memory remanence"* could be exploited to access data that have been left in Dynamic Random Access Memory (DRAM) even after power has been removed from the computer. This attack requires physical access to the computer hardware to either reboot the victim computer from a customized kernel or to briefly shutdown the computer and then start with a custom kernel. Another method would be to physically relocate the

[14] http://www.w3.org/TR/soap

RAM modules to the attacker's machine where it can be analyzed. Halderman *et al.* [43] illustrates that the decay of the data contained within these DRAM modules can be significantly delayed by cooling down the memory prior to removing power to the computer. In their experiments if the power was cut for more than one minute they were able to extract 99.99% of data from the cooled DRAM modules. The authors then demonstrate how to successfully defeat Bitlocker (Microsoft), FileVault (Apple), TrueCrypt, dm-crypt and Loop-AES by extracting the relevant encryption key and mounting the encrypted drive. Halderman *et al.* [43] also states that many users, who design and maintain systems that are to be deemed secure, are completely unaware of this threat, which compromises the fundamental integrity and confidentiality of information that has been encrypted with these technologies. The standards set forth by the client, with regard to the quality of the computing hardware and physical infrastructure (air conditioning, power supply and backups), may not be adhered to by the cloud provider [59].

Storage. Old storage media can be accidentally retired without client data being cleared. This scenario often plays out in cloud providers where there are no clear policies and procedures in place with regard to retiring storage media.

Hypervisor based threats. Assuming that one has full control over a rented virtual machine it would probably be a good idea to monitor it in some way. This is also true for the cloud provider who actually has much more control over a virtual machine, since the provider can monitor all the virtual machines on a particular host. Misuse of administrative privileges with a tool like *Xenaccess*[15] can allow an administrator to run a process to gain access to the memory of a client's virtual machine [26]. Similarly Szefer and Lee [87] also state that even hardened hypervisors are vulnerable to these memory based attacks. Szefer and Lee [87] also state that software such as *HyperSentry*[16] could be used for introspection (bypassing the hypervisor), which means that it could be used for malicious activities. Futhermore they state that many software based protection schemes can be subverted by attacking the virtual infrastructure from below (e.g., hardware based attacks). According to Szefer and Lee [87] this compromises the confidentiality and integrity of the guest virtual machines on the entire host, since the underlying hypervisor has been breached. An earlier example of a threat to the underlying virtual infrastructure was the use of *"the blue pill"*, which intercepts hardware calls made by the virtualized software running on the host [24]. To make matters worse *Xenaccess* comes packaged with a popular virtualization software package, called *Xen*[17]. Since some cloud providers have adopted *Xen* the possibly that a guest virtual machine may be tampered with is increased.

[15] https://code.google.com/p/xenaccess

[16] http://www.darkreading.com/applications/nc-state-ibm-researchers-create-stealth/227500269

[17] http://www.xen.org

Virtual networks, which allow the virtual machines to communicate with each other on the host and with the host itself, could also be monitored. This would allow the provider to gain insight into the traffic and information flowing through the virtual switch [26]. Thus having one compromised virtual machine puts all the others on the host at risk. This point of view is supported by Harauz *et al.* [44] where the authors claim that the cloud infrastructures present attackers with the opportunity to compromise several targets due to its inherent design characteristics.

Threats from other virtual machines. Just as physical networks could be subjected to packet sniffing and Address Resolution Protocol (ARP) poisoning, so can the virtual networks which virtual machines use for communication. It is also possible for malicious virtual machines to access other virtual machines via shared memory and networking resources [73]. This can even be done without compromising the underlying hypervisor. Memory deduplication, which is a method used by the hypervisor to reduce the amount of physical memory needed, is another method that could be used in attacks commonly referred to as *"memory disclosure attacks"* [86]. Differences in the write access times of the deduplicated memory pages are taken advantage of by this type of attack, which is then used to detect files and applications in other virtual machines. During experimentation Suzaki *et al.* [86] successfully detected the invocation of *sshd*[18] and *apache2*[19] on a Linux victim. However, they encountered problems when trying to detect Internet Explorer[20] running on a Windows XP (with service pack 3) virtual machine. The authors specifically mention that this attack vector should be taken seriously, since it does not violate any Service Level Agreement (SLA) statement pertaining to cloud computing. More importantly it is able to detect page views even on a network encrypted with TLS/Secure Sockets Layer (SSL). Subashini and Kavitha [84] state that the encryption of network traffic (via TLS/SSL) can prevent leakage of sensitive information. Thus, if successfully executed, this attack vector leads to the compromise of the confidentiality of information stored on the virtual machine. Yet another way in which a hypervisor based threat can be realised is via an inter virtual machine attack. Such an attack is described by Ristenpart *et al.* [72] whereby the authors execute cross virtual machine attacks via side channels (extraction). Their attack is based on the premise that the malicious virtual machine is resident on the same physical server as the target virtual machine (placement). This is determined by using network probing (using *nmap*[21], *hping*[22] and *wget*[23]). Once co-placement is confirmed, attacks can be mounted against the target virtual machine which results in the compromise of information confidentiality.

[18] http://www.openssh.com

[19] http://httpd.apache.org

[20] http://windows.microsoft.com/en-us/internet-explorer/products/ie/home

[21] http://nmap.org

[22] http://www.hping.org

[23] http://www.gnu.org/software/wget

Mobility of Virtual Machines. The movement of virtual machines to offline storage can pose security risks in that they can be corrupted or stolen without even touching the hard disk of the host. This raises issues regarding the confidentiality and integrity of the virtual machine images.

Denial of Service Attacks (DoS). This type of attack can allow a misconfigured virtual machine to consume all resources of the host, starving the other virtual machines [73]. Subashini and Kavitha [84] state that it is difficult to get assurance from SaaS cloud providers, as to the availability of their cloud-based applications, since their control has been outsourced to the provider. In a white paper authored by Wrenn [94] the author states that DoS attacks and others like it are examples of cloud abuse caused by (1) *"weak registration"* (2) validation protocols with *"popular"* third party cloud providers, (3) insufficient network security and (4) not isolating clients' cloud computing infrastructures.

Networking. IaaS implementations suffer from all the network related threats of the traditional and the virtual networks. These include, man in the middle attacks, Internet protocol address spoofing, port scanning and Distributed Denial of Service (DDoS) attacks [73]. Note that several of the threats listed have a direct effect on either the confidentiality, integrity or availability of the cloud-based information.

Although a discussion on the various cloud computing threats is important, it forms only one part of a larger threat model. For this reason a cloud adoption strategy should investigate how to mitigate such threats. In the following section the researcher will discuss several techniques and technologies which could be used in such a threat mitigation strategy.

2.6 Addressing Information Security Concerns in the Cloud

Several of the threats discussed in the previous section have a negative effect on the *"core"* information security concerns, namely the confidentiality, integrity and availability of cloud-based information. It thus makes sense to discuss how these threats affect these security concerns as well as possible countermeasures and mitigation techniques to address them. For the purpose of this study countermeasures are described by Saripalli and Walters [76] as a means to defend against,

> *"architectural and implementation mechanisms" [76, page 281]*

These mechanisms are then used to mitigate the vulnerabilities present in a system. Since the exploitation of a vulnerability (via an attack) leads to a realised threat one can understand why threat mitigation and countermeasures are important.

Unknown risks (see *Section 2.5*), as listed above, pose a general threat to the cloud and do not directly affect the confidentiality, integrity and availability of cloud services and data. The Cloud Security Alliance does however suggest that cloud providers fully disclose information relating to their (1) cloud infrastructure, (2) cloud data and (3) relevant logs. Wrenn [94] states that the cloud provider's operations should be transparent in nature with Choubey, Dubey and Bhattacharjee [16] adding that cloud providers should undergo accreditation and also be audited.

Confidentiality refers to the concern clients have with regard to the safety of their information and whether or not it is protected from unauthorized access [98]. It is stated by Pardeep *et al.* [55] that the very nature of cloud computing incurs great security concerns especially in terms of, amongst other things, data confidentiality. To some extent Ramgovind *et al.* [71] agrees by stating that confidentiality plays a big role in the control that organizations have over their information, especially in a public cloud. It is within public clouds that the multi-tenant nature of the cloud plays a vital role. This enables the data of multiple organizations to be located on the same physical host [70]. This, however, increases the risk that the unencrypted data, which could be contained in memory and on disk, and thus be accessible to other tenants on that physical machine. This multi-tenant nature of the cloud forms yet another reason why confidentiality is cited as a major adoption stumbling block [70].

Bradshaw, Millard and Walden [9] state that many clients will be concerned about what will happen to their data when their relationship or contract with their cloud provider comes to an end? Clients may ask the following three questions:

- Will the data stay confidential up until such a time that it is removed?
- How long will it take for the cloud provider to remove the data?
- Will it be possible to access or port the information to another system?

According to Bradshaw *et al.* [9] Amazon[24] and ElasticHosts[25] contracted clients should be able to retrieve data from them up to thirty days after the contract comes to an end. In fact according to Zizzis and Lekkas [98], *"data remanence"* could lead to the unintentional compromise of data confidentiality, thus requiring special attention when terminating a contract. The requirement of a university in terms of this *"grace period"* may vary greatly

[24] http://aws.amazon.com

[25] http://www.elastichosts.com

and is largely up to the views of university key stakeholders. Even with confidentiality listed as one of the top three concerns, some cloud providers make data confidentiality the client's responsibility, as is the case with IBM Smart Business Cloud[26] [9].

There are a number of possible solutions to mitigate the threats that may lead to the compromise of cloud-based data confidentiality. According to Harauz *et al.* [44] three general capabilities should be on offer from cloud providers to ensure, amongst other things, confidentiality of information:

- **Encryption of data**: The Cloud Security Alliance [20] states that cloud providers should secure any data in transit via encryption as well as perform inspection of the said network traffic. They further state that practices involving the generation of strong encryption keys, deletion of cloud-based data and management of data storage be strictly adhered to.
- **Backup of data**: Subashini and Kavitha [84] state that cloud providers should backup sensitive data making sure that these backups are encrypted to prevent data leakage. The Cloud Security Alliance [20] and Choubey *et al.* [16] propose that customers contractually specify that their cloud-based storage be completely formatted (before being re-used by the provider) and that the conditions surrounding cloud-based backups be clearly stipulated.
- **Prevention of unauthorized access to data**: The Cloud Security Alliance [20] states that customers should make an effort to comprehend what is communicated within the cloud provider policies, as well as the SLA they have with the provider. Choubey *et al.* [16] states that the SLA, between the customer and cloud provider, be precise in its break-down for what each party is responsible. The conditions for dissolving a contract is also of significant importance. The Cloud Security Alliance [20] recommends that two-factor authentication be employed, the cloud infrastructure be actively monitored and that credentials not be shared. Wrenn [94] agrees that the cloud should be monitored by the provider, but that sufficient reporting on any changes to the cloud also be available.

In addition to the general capabilities listed above, virtualization is listed by Armbrust *et al.* [2] as the primary security mechanism in cloud computing. Armbrust *et al.* [2] however admits that the improper configuration of a virtualized environment can lead to several security issues such as unauthorized access to other users' information or resources. All of which undermine the confidentiality of the information that is stored in the cloud, as discussed in the previous section (virtualization-based threats).

[26] http://www.ibm.com/cloud-computing/us/en

In a virtualized environment there are several ways in which one could appease threats to the confidentiality of cloud-based information. Szefer and Lee [87] suggest using the *HyperWall* architecture to achieve what they call *"hypervisor-secure virtualization"*. Confidentiality and integrity protection tables are key features of the *HyperWall* architecture, which enables it to secure all the information within a specific virtual machine's memory. Another solution is *Trusted Virtual Datacentre*, which looks at securing the virtual datacentre from an infrastructure and management point of view [26]. To get a solution that is directly in line with the security concerns that need to be addressed, one could look at *Trusted Cloud Computing Platform (TCCP)*. In TCCP closed box execution is provided and confidentiality and integrity of computations is ensured [26]. Unlike other mitigation technologies the latter two solutions can function in a complex virtual infrastructure.

In an effort to reduce the risk of data leakage Puttaswamy *et al.* [70] propose a system called *Silverline*, which identifies all the data that can be functionally encrypted, assigns encryption keys to subsets of data to minimize the complexity of key management. This provides robustness in case of key compromise. Puttaswamy *et al.* [70] states that *Silverline* achieves all of the above without causing operational hindrance. This encrypted data would then only be accessible to users who are in possession of valid keys, which ensures the confidentiality of cloud-based data. Puttaswamy *et al.* [70] also suggest that cloud providers should never be given access to any unencrypted data. Similarly Xiong *et al.* [95] suggest that the content provider (client) should store the cryptographic keys out of the reach of the cloud provider. An example of a cloud provider that does not give administrators access to the guest virtual machines is Amazon EC2.

Yet another system that ensures the confidentiality of information in the cloud is *CloudSeal*, which also makes use of symmetric encryption [95]. The authors Xiong *et al.* [95] recognize the shortcomings of earlier proxy-based encryption with regard to the frequent key revocation problems as found in cloud-based data sharing systems. Assuming that the client has contracted a semi-honest cloud provider, which is the case with most providers, *CloudSeal* guarantees stronger security of the content together with improved user and key management. Clients are however warned by Puttaswamy *et al.* [70] that encryption should not be used naively, because it can limit the usage of the cloud-based data, since computations in the cloud can only be performed on plain text data. Zissis and Lekkas [98] propose that confidentiality be addressed by using a trusted third party, which will be responsible for assuring the security of the cloud environment. Of course this sounds familiar, since this is the principle on which certificate authorities operate. Ristenpart *et al.* [72] states that the client should be given the choice of where they want to place their virtual machine in order to ensure the confidentiality of their cloud-based information. They state that cloud providers should obfuscate the internal structure of their clouds to make it more difficult to map as well as employ blinding techniques in order to hide the services running within the cloud providers' cloud infrastructure.

To reduce the threats users face with regard to *"memory remanence"* attacks, Halderman *et al.* [43] suggests that:

- The computer be powered off completely and that the user then waits a minute or two so that the memory can decay sufficiently,
- Cryptographic pre-computations (to speed up cryptographic operations) should rather be performed as needed,
- Computer manufacturers could employ technologies such as Intel's *Trusted Platform Module*[27] purpose built (soldered onto the motherboard) to store cryptographic keys.

Halderman *et al.* [43] states that many Trusted Computing hardware does not prevent these memory based attacks and are thus largely ineffective in reducing the threats realised via these attacks vectors.

Information integrity forms another integral part of the triad of information security. Zissis and Lekkas [98] define it as follows:

> *"The protection of information either locally stored or in transmission from unauthorized access." [98, page 588]*

To ensure that a cloud provider will guarantee the required integrity, one could start by inspecting the terms and conditions carefully. The survey that was conducted by Bradshaw *et al.* [9] found that some cloud providers, for example Rackspace[28], would only guarantee the integrity of the client data if they purchased additional backup services. On the other hand Symantec[29] and Iron Mountain[30], who do offer backup services, did not mention information integrity in their terms and conditions at all. To illustrate this point an excerpt from the disclaimer of Amazon Web Services[31] is supplied:

> *"AWS has the right but not the obligation to monitor and edit or remove any activity or content. AWS takes no responsibility and assumes no liability for any content posted by you or any third party."*

In [93] it is mentioned that virtual machine images should have high integrity, because the images determine the initial running state and its security. The authors go even further by claiming that the security of the images

[27] http://www.intel.com/support/motherboards/server/sb/CS-032413.htm

[28] http://www.rackspace.com

[29] http://www.symantec.com

[30] http://www.ironmountain.com

[31] T&C: http://aws.amazon.com/terms (Last accessed: 9th of June 2012)

determines the security of the cloud infrastructure. One solution proposed by Wei *et al.* [93] is the use of an image management system called *Mirage*. They claim that most cloud providers only focus on the running instances of the images, but not those that are dormant. *Mirage* consists of an access control framework, image filters, provenance tracking and repository maintenance services, all of which enhance the security and integrity of the dormant virtual machine images [93].

Availability is the property of a cloud service or application that makes it usable and accessible by authorized users of the cloud environment. According to Zissis and Lekkas [98] system availability is the ability of the system to still be able to function even if some of the authorities do not behave as expected, as is the case with security breaches. Because the network is used for the retrieval and processing of the cloud-based information, it is the cloud provider's responsibility to guarantee that the client's information, and the processing thereof, is available on demand [98]. Similarly Subashini and Kavitha [84] state that clients should be provided with access to cloud services at all times, requiring the cloud provider to make changes to the application and infrastructure architecture. This can be achieved by utilizing server farms, using resilient software/hardware and having proper disaster recovery and business continuity plans in place. Molnar and Schechter [59] state that under provisioning, which could undermine the availability of cloud services, could be mitigated by attestation-based mechanisms used for auditing. These mechanisms could be used to ensure that capacity has been provisioned to levels equal to that which was agreed upon in the SLA.

To limit the damages caused by DDoS attacks, Molnar and Schechter [59] suggest the use of resource quotas. The Cloud Security Alliance [20] states that cloud providers ensure that utilized network blocks are not blacklisted. If blacklisted this could result in the unavailability of cloud-based services; affecting many customers due to the multi-tenant nature of the cloud.

Just because a cloud provider claims it can do something it does not follow that it is capable of delivering on that promise. This specific claim is usually closely related to the SLA that is negotiated with the cloud provider. In fact this is exactly what Cachin, Keidar and Shraer [13] suggest, where they implore clients to understand the service level agreement that they have with their cloud provider.

In an effort to reduce standard DDoS attacks, Amazon makes use of synchronous cookies and connection limiting [84]. They do this by ensuring that their internal bandwidth exceeds that of their actual Internet bandwidth. Reducing access rights, keeping software updated and closing any unused ports is often overlooked in favour of more elaborate availability solutions. Keeping the network up and running is vitally important to be able to deliver a reliable cloud service. Basta and Halton [4] suggest that encrypted protocols be used and that changes to ARP tables should be logged.

Another system that has been proposed by Bowers, Juels and Oprea [8] is the use of High Availability and Integrity Layer (HAIL) to improve file availability of storage systems; in this case cloud-based storage. HAIL is unique in that it combines two approaches namely, Proofs Of Retrievability (POR) and Proofs of Data Possession (PDP), these approaches in the past were used in isolation. It is thus essential that a cloud provider be chosen that will be able to deliver on the promises made in their SLA. Along the same lines it is also important for the client to accurately judge how any lapses in availability will affect their organization.

Since, as Monfared [60] suggests, security concerns about the confidentiality, integrity and availability of cloud-based data has been the main driving force behind the *"slow uptake"* of the cloud it becomes important to know what the threats are and how one can possibly mitigate them.

The discussions above illustrates several techniques and technologies which could be used to address threats to the confidentiality, integrity and availability of cloud-based information. Although threat mitigation forms an integral part of a successful adoption strategy it is unlikely that all the possible threats could be thwarted. As such it is imperative that cloud providers and subscribers understand how to react to security incidents arising from realised threats. For this reason the next section discusses the various phases of the security incident response life cycle.

2.7 Security Incident Response in the Cloud

From *Section 2.6* one can see that a realised threat is the result of an attacker exploiting some known vulnerability of a system. This attack then leads to a security incident. A computer security incident can be defined as,

> *"...an incident is a violation of computer security policies, acceptable use policies, or standard computer security practices.." [63, page 65]*

Knowing exactly how an organization will respond to an incident in the cloud is an important part of the cloud computing adoption process. To ignore this, knowing that there is a large amount of security concerns, would be tantamount to planning to fail. The incident response life cycle is illustrated in *Figure 2.2*, around which the discussion about security incident response will be based.

The Cloud Security Alliance provides the following reason for planning incident response:

> *"Even the most diligent planning, implementation, and execution of preventative security controls cannot completely eliminate the possibility of an attack on the information assets." [19, page 93]*

Organizations should thus be looking at how they could adapt their current incident response strategies with the cloud model that they intend to adopt. In the event of an incident, the very nature of the cloud and its elasticity, as well as on-demand capabilities may have an effect on the amount of help that can be expected from the cloud provider [19]. The Cloud Security Alliance specifies that the detection, analysis, containment and recovery from a security incident should be discussed with the cloud provider during the planning stages of a formal incident response plan. Grobauer and Schreck [42] state that if provisions for incident handling are not arranged with the cloud provider, incident handling will become difficult, if not impossible, for the client.

Another factor that impacts on incident response is the ineffectiveness of forensics, since it relies on aspects that are influenced by resource pooling at the cloud provider [19, 42]. In the event that some form of information is gathered on an incident, resource pooling could cause privacy issues. Especially since co-tenant information may be included in the incident logs. Jurisdictional boundaries could impact possible responses to incidents, since different geographical regions might not allow for the sharing or acquisition of forensic data.

The statements above make it quite clear that not planning a *"security incident response plan"* could have many negative effects on the cloud-based data of the organization. In order to understand how security incidents in the cloud can be planned and dealt with effectively, one needs to investigate the security incident response life cycle as depicted in *Figure 2.2*. To accomplish this all the phases of the security incident response life cycle are discussed in *Sections 2.7.1* to *Section 2.7.5*.

2.7.1 Security Incident Preparation

The first step in the incident response life cycle contains the following collection of actions, as recommended by Grobauer and Shreck [42]:

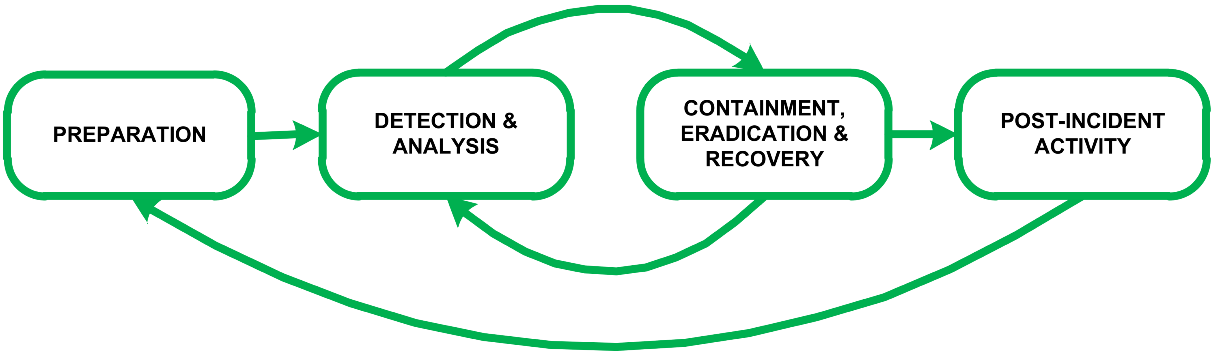


Figure 2.2: Security incident response life cycle (adapted from NIST [63])

- It is the most important aspect of creating an incident response plan and should be done prior to anything else, especially before migrating to the cloud.
- If there is no expertise in an area of necessity, a suitably qualified external party should be involved.
- At all times the planning should be performed where the data is located.
- Should the incident involve different jurisdictional boundaries, the creation of data flows between geographic areas and physical assets could assist in planning incident response.

Alternatively the SANS Institute [75] suggests that an organization clearly defines the types of incidents. Defining these will make it easier for the cloud provider and client to negotiate service level agreements. Mission statements of the cloud provider and the client could be used during the incident preparation phase [75]. Priorities exhibited in the mission statement will dictate how the cloud provider communicates, which in turn affects the client [75]. The following list of preparations deals with the service level agreement between the cloud provider and the client and forms an integral part in the planning process, since both parties need a clear understanding of what is expected from each other in the event of a security incident. When outsourcing services or applications to a cloud provider, the cloud subscriber should make sure that the cloud provider articulates how the service level agreement will address the following items:

- Where to call, and to whom to speak in the event of an incident [75].
- Definition of incidents and notifications from both the cloud provider to the client and external parties, if involved.
- The type of support the cloud provider will extend in terms of the type of logs and incident information being provided.
- Roles and responsibilities of both parties during a security incident.
- Another important aspect is the testing procedures and specifications of possible incident responses.
- What kind of reporting will be provided after the incident has taken place and the amendments to the SLA with regard to the solution of the incident, if required.

The SANS Institute [75] also adds:

- Those members of the incident response team might need training to work with virtual machines or with the self-service portal, if one is provided.

- Is there a legal requirement to disclose breaches in security to the media? If the cloud provider is required to make incident information available how will they go about doing so? Will the client be notified first?

It is also important to note that cloud deployment and delivery models will greatly influence the preparation phase, since some areas will either be out of the client or the cloud provider's control. This is yet another good reason to ensure that these differences and expectations are clearly stipulated in the service level agreement.

2.7.2 Sources of Security Incident Data

From *Figure 2.2* it is clear that this topic is not represented in the security incident response life cycle. It does, however, warrant a place in this discussion because without any relevant incident data no proof of an incident can be found. According to the Cloud Security Alliance [19] it is important for the client's Incident Response (IR) team to determine what type of logging and how much logging will be required by their applications. If not done appropriately logs might not contain information of any value when incidents do occur. Also, will these logs be made available by the cloud provider? The following list compiled by the Cloud Security Alliance [19] contains all the possible questions to ask and to plan with regard to the logging of security incident data:

- Which information should be logged?
- Is the logged information complete?
- Do the logs exhibit the dynamic nature of the public cloud?
- Are the logs being collected, tamper proof or just tamper resistant?
- Do the logs conform to any legal requirements that there might be?
- What retention periods should be address?
- How are logs transferred to the client and in which format?

Its is obvious then that these questions and answers should be dealt with during the preparation phase of the incident response life cycle. During the preparation phase provision should be made in the service level agreement as to what is to be logged and how the cloud provider will be involved with the gathering and analysis of security incident data sources [19].

2.7.3 Security Incident Detection

The different cloud models all require a varied approach to how incidents are detected and analysed for that matter. According to the Cloud Security Alliance [19] the detection of security incidents in the cloud depend on the following three aspects:

- That existing event logs are monitored sufficiently,
- Systems that focus on security events (i.e., intrusion detection and prevention) should be added as soon as possible, and
- The methods that identify events indicating an underlying security incident has been perfected and implemented.

The following additional detection aspects are added by the SANS Institute [75]:

- Whether or not the cloud provider actively monitors and patches vulnerabilities reported by information outlets, especially for Commercial Off-The-Shelf (COTS) information outlets. An example would be the NIST[32] outlet where some cloud providers are already starting to appear.
- Attention should be given to incidents reported by staff members of an organization, who may report an obvious security incident. This then gets reported to the helpdesk.

In addition to the dependencies above, the following customer related security incident characteristics play a vital role in the detection process:

No access to the cloud provider's security and vulnerability information. This is most severe in SaaS and PaaS environments. IaaS environments have more control, because the virtual machine is under the control of the client. The Cloud Security Alliance [19] suggests that access be provided to clients and that options relating to this be explored in service level agreements.

Inadequate interfaces to interact with security incident information. Once again SaaS and PaaS environments will be dependent on the interfaces provided by the cloud providers. Open interfaces should be implemented, which are at the heart of responding in a timely fashion to security incidents [19].

[32] http://nvd.nist.gov

Not possible to add event sources relating to security. Firewalls, intrusion detection and prevention systems are almost impossible to add to specific sources of security events, especially in SaaS and PaaS environments. Intrusion detection and prevention, and any other beneficial SaaS offerings can be offered as a service add-on by the cloud provider [19].

Incorrect recipients of security incident reports. Incident reports that are supposed to be sent to the client might be sent to the cloud provider. Cloud providers should therefore be open to the possibility of receiving security incident reports and notifications from third parties. These should then be communicated to the clients in a manner defined in the service level agreements [19]. The SANS Institute [75] states that additional questions during the preparation and planning phase need to be asked with regards to the level of incident reporting by the cloud provider in terms of what is reported and to whom.

2.7.4 Security Incident Analysis

The analysis of incident information or data is a real challenge in cloud computing environments due to the dynamic nature of the cloud infrastructure. What type of incident information is available and how does the client interpret the results are questions that need to be addressed.

The cloud provider may not make sufficient amounts of information available. It may not be in a format that the client can interpret with any useful results. Their use of proprietary software and hardware makes incident analysis difficult for cloud subscribers. To develop a closer relationship with the cloud provider Durkee [31] suggests that the configuration of the cloud provider's architecture be provided to the client, even if that requires a non-disclosure agreement. The Cloud Security Alliance [19] also states that there are no guidelines on how to conduct a successful digital investigation that will gather credible information. This together with the absence of legal cases concerning security incidents in the cloud and adequate guidelines might make the evidence inadmissible in a court of law [19].

Cloud computing has introduced many technical advances, which has made gathering and analysing information security incidents difficult. This is especially true of SaaS and PaaS environments where machines are shared and event logs contain information not belonging to only one client [42]. Grobauer and Shreck [42] extend this aspect of security incident analyses by stating that the limited architectural information of the cloud provider will limit the analyses that the client can perform. Detailed knowledge of the network architecture and applications are needed to analyse security incidents successfully. The SANS Institute further states that lack of visibility in terms of how the infrastructure of the cloud provider is organized complicates incident response teams tremendously. The Cloud Security Alliance [19] suggests that clients:

- Ensure that they have access to the data that relates to information security incidents and that,
- They have the needed forensic support from the cloud provider to be able to analyse these forensic datasets in a meaningful manner.

Ignorance of relevant security incident information sources and ignorance of the cloud provider infrastructure also impacts on the analyses of security incidents in the cloud. According to Grobauer and Shreck [42] defining the responsibilities of the cloud provider and that of the client is also of vital importance when it comes to the analyses of security incidents. To make the analyses of security information easier, especially in the context of what was discussed above, Grobauer and Shreck [42] suggest the following:

- Access should be provided to the cloud provider's infrastructure,
- Cloud provider to provide access to relevant security incident information, and
- Use of forensic capabilities of the virtualization infrastructure of the cloud provider.

2.7.5 Security Incident Recovery

After thorough incident analysis has been performed the client or cloud provider must investigate possible means to recover and eradicate the security incident. This could be a malicious program, inside attack or misuse of administrative privileges. Grobauer and Shreck [42] further state that it is difficult to give general advice in this area and that it would be more productive to illustrate with real world security incidents. It should also be noted that the Cloud Security Alliance [19] suggests that the process of security incident recovery and eradication be done with minimal disruption to the business and that legal and privacy implications be taken into account. The Cloud Security Alliance also state that different cloud deployment and delivery models will have different recovery, containment and eradication strategies.

Planning for security incidents is thus of utmost importance and should be done during the incident preparation phase. Another aspect that should be discussed with the cloud provider is exactly how the cloud provider intend on dealing with security incidents on their infrastructure. This is especially important, since this infrastructure will most probably be multi-tenant in nature. Recovery, containment and eradication could thus affect multiple clients [19], inadvertently placing control of the situation outside the hands of the client. Similarly Grobauer and Shreck [42] state that a security incident that affects the cloud provider's infrastructure is completely outside the control of the client and cannot be investigated.

For IaaS clients recovery, containment and eradication could actually be easier in a public cloud, since their virtual machine images could be paused and moved to another cloud where the recovery processes can be performed in relative safety [19]. The isolation of a compromised server would usually be done by severing all network connectivity, but Grobauer and Shreck [42] on the other hand suggest that this will depend on how the cloud providers network is configured.

Both the Cloud Security Alliance [19] and Grobauer and Shreck [42] agree that the use of virtualization offers the advantage of preserving the compromised machine, which enables a full forensic investigation. Starving a compromised machine of resources is also a lot easier in a virtual environment and can be effectively used to contain security incidents. One example might be the mitigation of a DDoS attack, which is a resource intensive attack [42]. Cloud providers should be able to help the clients with some security incidents for example DDoS attacks [19], but according to Grobauer and Shreck [42] they should go two steps further by providing:

- The ability to configure the networking of the virtual infrastructure at the cloud provider and
- Having access to snapshots of the affected virtual machines and manipulation thereof.

Clients in SaaS and PaaS environments are usually exposed to vulnerabilities in the software that compromises the integrity and confidentiality of the information stored and/or accessed by the client on those cloud delivery models. According to Grobauer and Shreck [42] web application firewalls can be employed to prevent exploitation of the vulnerability whilst the cause of the actual security incident is tracked down. Grobauer and Shreck [42] state that containment depends greatly on:

- The granularity of the access rights that can be assigned from within the application and
- Whether or not there is a possibility to implement certain workarounds.

Eradication in a PaaS and SaaS environment is definitely supposed to be done by the cloud provider, but the client should also perform certain duties from their side, like removing the data from the compromised application [42]. Understanding the incident response life cycle and how the various delivery and deployment models fit into the cycle is of utmost importance. From the discussion above it appears that the use of some delivery models needs more co-operation from the cloud provider and subscriber. Security incident response is all about planning and knowing what to do and how to do it when needed. This planning process should be done in cooperation with the cloud provider, which can actually aid the client in choosing a suitable cloud provider.

As highlighted in the above discussions it is imperative that both the cloud provider and subscriber be involved in every phase of the security incident response life cycle. It further indicates that this involvement should not only be limited by each party's participation, but should also include articulating what the cloud provider and subscriber are responsible for during the execution of these phases.

2.8 Adopting the Cloud

Although there are a myriad of information security threats, and traditional security concerns surrounding the adoption of cloud computing, many organizations are making a move towards the cloud. Evidence that cloud adopters are indeed satisfied with the move towards the cloud can be found by studying the results of the survey completed by Appirio in 2010 [1]. During this survey of medium to large (500+ employees) organizations 60% of participants (General Managers, Managers, Vice-Presidents, Directors) agreed that they have achieved greater levels of availability by adopting the cloud. This survey also confirmed that organizations are mostly not using the cloud to save costs, but rather to achieve greater business agility, with 83% agreeing that the cloud will allow them to respond faster to business needs. Similar results were obtained in a 2011 survey by Deloitte [27] where businesses (from Belgium, France, United Kingdom and the Netherlands) were taking the lead in adopting the cloud, citing the following as the main reasons for doing so:

- Flexibility,
- Cost,
- Accelerated Deployment, and
- Better Functionality

Only 20% of participants cited data security as a reason to not adopt the cloud. Deloitte [27] found that many business leaders are subjected to large amounts of data from vendors about cloud computing, which is not always clear. This leads to confusion on their part, which is confirmed by their lack of knowledge with regard to the specific cloud offerings by popular cloud providers. Similar findings were reported by f5 Networks who conducted a survey of 250 companies in 2009. Participants in their study were employed in the following capacities: Manager, Director (no CIO's), Vice-President and Senior Vice-President. f5 Networks state that,

> *"... significant confusion regarding the definition of the cloud exists,..." [36, page 3]*

This confusion has lead to the fact that many businesses are hosting critical applications in-house, as found in the study by the Ponemon Institute [68]. According to them only 16% of European and 21% of American participants (Information Technology practitioners from Europe and America) are currently hosting critical business applications in SaaS clouds. Additionally 42% believe that cloud providers are responsible for securing SaaS resources. American-based practitioners cited almost exactly the same reasons for adopting the cloud as the European businesses surveyed by Deloitte [27].

However, in Europe and the US only 14% stated that adopting the cloud will lead to an increase in security. The survey also found that 69% of participants believe end users are responsible for a safe and secure cloud environment, with 64% believing that business is responsible for a safe and secure cloud experience. Most important factors affecting their organizations overall security was listed as not knowing where the information is physically located (US) and not being able to limit physical access to the cloud infrastructure (European). Another aspect of the survey is that participants were most confident in the cloud when determining the root cause of cyber attacks as well as a means to prevent system downtime.

Although clients are not able to control network intelligence systems housed within a cloud provider's infrastructure, 64% of participants still rated it as the most effective means of protecting a cloud infrastructure.

2.9 Concepts Revisited

In the previous discussions the reader was presented with an overview of cloud computing, which included an analysis of any associated threats to the security of cloud-based information. The researcher also made reference to security incident response by discussing the specific phases of the security incident response life cycle. The fact that many of these examples and surveys focus on businesses, makes their results inadequate to address the challenges faced by institutions of higher education, because of differing security and operational contexts.

From the literature the researcher infers that South African universities will be faced with several information security concerns when looking towards adopting the cloud. The literature further illustrates that there are a myriad of theoretical systems (i.e., *Silverline*, *Cloudseal* and *HAIL*) and threat mitigation techniques to address concerns surrounding the confidentiality, integrity and availability of cloud-based information.

One is also confronted by surveys such as those conducted by the Ponemon Institute [68], Data Security Council of India [25], Deloitte [27], Appirio [1] and f5 Networks [36] which confirm that the information security concerns

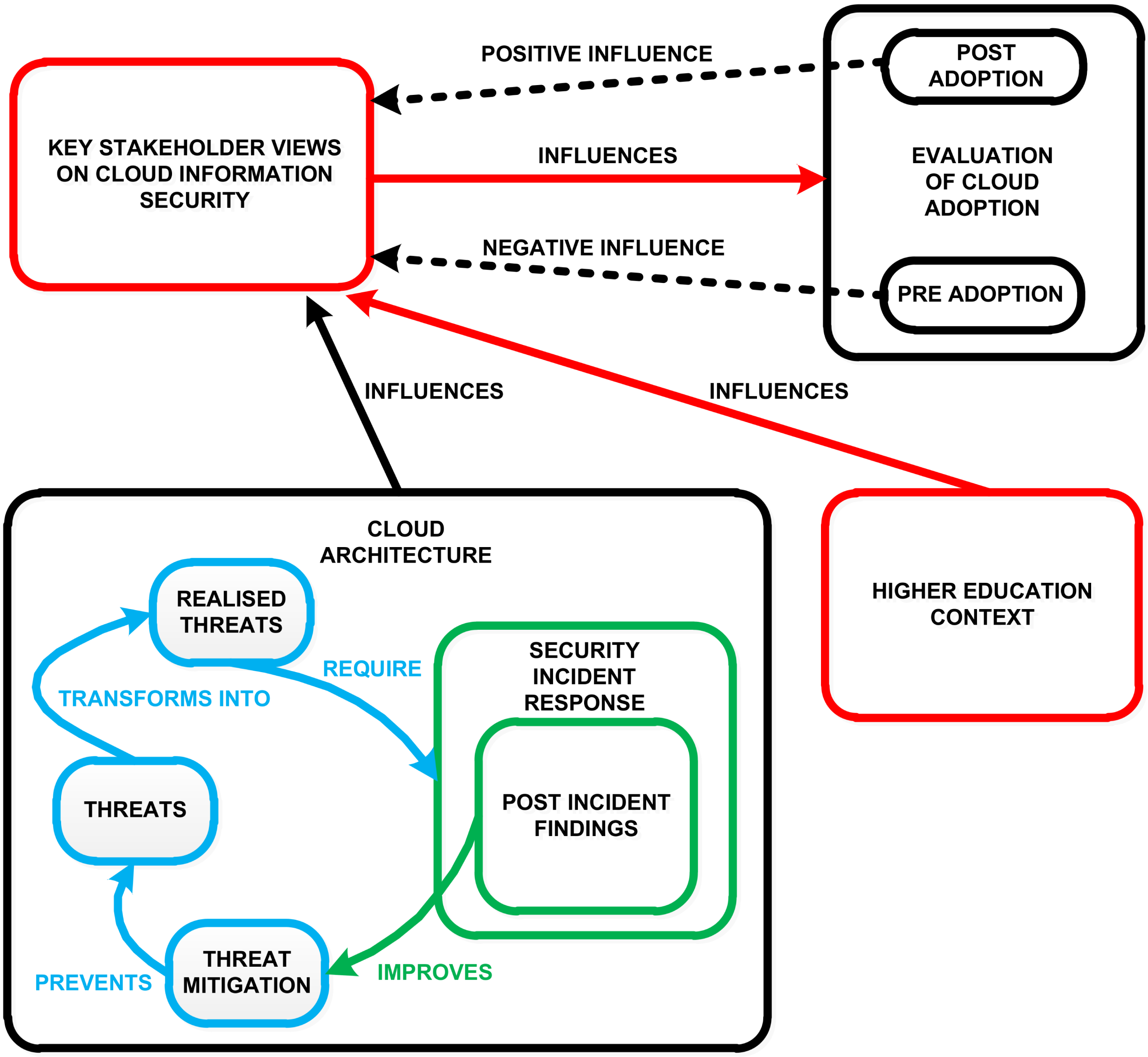


Figure 2.3: Core concepts in literature review

and their relation to cloud adoption have a direct affect on organizations. Documentation like those provided by the SANS Institute [75], Cloud Security Alliance [19, 20] and NIST [64] allows for the exploration of even more theoretical advice and best practices, but do not address how key stakeholders view cloud information security.

The information above together with the fact that most of these surveys and studies was conducted within a positivist framework, highlights various knowledge gaps. This is further exacerbated by the lack of any existing studies on the specific needs of South African universities. As such this study sets out to investigate a subset of these knowledge gaps (see the research questions in *Chapter One*) within an interpretivist framework.

To assist in the investigation the researcher constructed a conceptual framework, as illustrated in *Figure 2.3*. This framework not only illustrates the core concepts contained in the literature review, but also provides this study with a conceptual lens to aid in the data collection process. Most importantly it depicts the researcher's theoretical understanding of how these concepts relate to each other. On the left of the conceptual framework threats, realised threats, threat mitigation and security incident response is illustrated (see *Sections 2.5 to 2.7*). The researcher would like draw the reader's attention to the grouping of these concepts, which is indicative of the relationships they have with each other.

Although the literature does not distinguish between a threat and a realised threat the researcher felt the need to include this concept here, since it could result in a security incident. To effectively address a realised threat some form of incident response is required. If the incident response life cycle is followed, it is the last phase (post incident findings) which could then be used to improve threat mitigation, since it offers key universities the opportunity to learn from these realised threats. This in turn improves threat mitigation, which prevents this specific type of threat from taking place again. The researcher not only connected the concept of a threat and a realised threat, because a threat transforms into a realised threat, but more importantly also because it is impossible to mitigate for every conceivable threat. For this reason the conceptual framework depicts a cycle between the concept of a threat and security incident response. These concepts are also related to cloud architecture (see *Section 2.2*), since the type of cloud service and deployment model determines the threats it is exposed to, as well as how to deal with security incidents within this context.

In the upper left corner of *Figure 2.3* the views of key stakeholders are depicted. Importantly the literature only contains the views of key stakeholders outside the context within which institutions of higher education operate. Many key stakeholder views are further restricted by the limited information which was gathered by these surveys. Some of the results from these surveys are discussed in *Section 2.1 and 2.8*).

The fact that these surveys did not focus on universities is indicative of a knowledge gap, especially in terms of an in-depth study into key stakeholder views. Surveys, such as those conducted by Appirio [1], found that these views differ depending on whether the cloud subscriber is still evaluating the cloud (pre-adoption) or has already adopted it (post cloud adoption). This is indicated by the relationship between these views and cloud adoption. These views are then either positively or negatively influenced, depending on whether or not the subscriber has or has not adopted the cloud.

With context playing such a central role in this study the researcher included it in this framework; even though it is mostly discussed in *Chapter One*. More importantly it also addresses the second part of the overarching knowledge gap in the sense that most of the studies on cloud computing have been positivist in nature, which excluded the context of the participating organizations. It is anticipated that the context within which South African universities operate together with their chosen cloud architecture directly influences their views on cloud information security.

It is these concepts and their associated relationships that will form the basis of the initial data collection instruments; namely the online survey which is discussed in the following chapter.

2.10 Summary

In this chapter the reader was provided with an architectural overview of cloud computing. Several reasons to adopt cloud computing were listed together with a discussion about the technologies that make cloud computing possible. This was followed by a detailed discussion on cloud computing threats and the techniques, as well as the technologies to mitigate their effects on the confidentiality, integrity and availability of cloud-based information. Thereafter the reader was presented with a discussion on the various phases of the security incident response life cycle, detailing the procedures cloud subscribers should follow in order to ameliorate any realised threats. This was then put into perspective by investigating several surveys that set out to gather information on how other organizations have reacted to questions about the security of cloud-based information as well as cloud adoption.

The chapter concluded by presenting the reader with a conceptual framework wherein the researcher's understanding of the core concepts in this study are illustrated. It is in *Chapter Three* that this framework will be used to guide the construction of survey questions.

Chapter 3

Methodology

3.1 Introduction

In *Chapter One* the researcher formally specified the research questions of this study. It is anticipated that answers to these questions would afford the researcher the opportunity to understand the views of key stakeholders with regard to cloud information security. In addition to these research questions *Chapter Two* also identified areas that have not been researched. These were not only limited to the type of organizations studied, but also highlighted gaps in how they were studied culminating in a conceptual framework to further guide this study within an interpretivist paradigm.

This chapter takes this methodological motivation a step further by detailing the various research design elements together with their practical implementation. In essence it provides a detailed plan of how the researcher will be executing this interpretive research.

Chapter Three will commence with a discussion on the research paradigm (see *Section 3.3*) followed by the research methods and data sources that are to be used (*Sections 3.4* and *3.5* respectively). In *Sections 3.6* and *3.7* the reader will be presented with detailed information regarding the data collection methods as well as the type of data that is to be collected. *Section 3.8* will conclude this chapter by detailing how thematic analysis will be used in the analysis of the data generated by the in-depth interviews.

3.2 Terms and Definitions

The following terms and definitions have been provided to assist the reader in understanding the core methodological components of this study.

Data Corpus: A term that refers to all the transcribed in-depth interviews that were conducted during this study.

Data Extract: Refers to pieces of a data item that has been coded (i.e., sentences, phrases or short paragraphs).

Data Item: The term data item refers to a single transcribed interview.

Data Set: A data set is a collection of either data items or data extracts that share a common analytical trait.

Key Stakeholder: University employees who are in senior IT management or administration. These would be the following: IT Managers, Technical Managers, Operations Managers, IT Directors, Systems Managers and System Administrators.

Latent Theme: A theme that goes beyond the semantics of the data itself. Latent themes are concerned with the identification and close inspection of the intrinsic ideas, assumptions and concepts that define a theme, which tends to favour an interpretive approach for analysis [10].

Semantic Theme: A theme that presents itself in what is apparent from the raw transcribed data. With a semantic theme the researcher makes no effort to interpret the data any further than what was said during an interview [10].

3.3 Research Paradigm

As stated by Schwartz-Shea and Yanow [96, page 23] interpretive research targets context-specific meanings. It is exactly this focus on the meaning of key stakeholder views as well as their contextual characteristics, situatedness and the situatedness of knowledge holders (researchers and participants alike) that forms an innate part of interpretive research; one that differentiates it from positivist research [96, page 32-33]. According to Klein and Meyers [53] interpretive research enables a researcher to comprehend how humans think and act within their respective socio-organizational contexts. The authors further state that it has the capability to generate a profound comprehension of the phenomena produced in the context of an information system. Walsham formalizes this by stating that interpretive research methods are,

> *"... aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" [91, page 4-5]*

From a philosophical perspective this interpretive study is based on the concept that multiple socially created realities exist. It is assumed that through language, participants of this study experience and construct their own social reality [61]. Thus, within an interpretive study participant's reality is socially constructed. Social reality forms an integral part of the nature and use of these mediums, which Morgan and Smircich refers to as *"modes of symbolic action"* [61, page 494]. Meaning is created by placing themselves (researcher and participants) within their own and each others worlds or contexts. Any differences encountered during the in-depth interviews are not seen as flaws in the data (positivist presupposition), but rather as interesting avenues for further research. This indicates that the participants have attached different meanings to the same concepts discussed during the in-depth interviews [96, page 41]; affording a researcher the opportunity to understand the different meanings given to the concepts discussed during the acquisition of knowledge. The researcher does this by investigating and analysing the various interpretations of the interview participants [96, page 41].

From the above it follows that the philosophical foundations of this interpretive study are:

- Knowledge does not exist separate from the context in which it is used. This applies to the research participant as well as the researcher and often requires the researcher to contextualize by reflecting,

  > *"on the social and historical background" [53, page 72]*

  of the case under investigation.

- The meaning attributed to a point of view or a perception of a participant might change over a period of time and may also differ depending on the location of the research participant or researcher. Knowledge is thus intrinsically situated.

- Participant experience and social factors greatly influence the meaning they attribute to the concepts explored as well as the views and perceptions formed during the social engagement [53],

- For this reason multiple socially created realities exist.

In addition to these philosophical aspects, this study will also apply a number of principles specifically related to interpretive field research. Of the seven principles mentioned by Klein and Myers [53] the researcher applied the following principles during this study.

The Fundamental Principle of the Hermeneutic Circle: Understanding will be achieved by moving between the meaning of the individual parts (concepts) as well as the whole that form (themes) within the operational context of each participating university.

The Principle of Contextualization: This principle will be used to show the reader how the social background of the participants and the research setting influences the researcher's interpretations.

The Principle of Dialogical Reasoning: During this study certain findings may contradict the theoretical concepts and frameworks set forth in this study, which requires sensitivity from the researcher's perspective.

The Principle of Multiple Interpretations: During the execution of this study the researcher should be aware that multiple interpretations of the same data may exist. This pertains specifically to the multiple interpretations participants may have with regard to cloud information security and the factors that influence it.

The Principle of Suspicion: The researcher should also be aware of the possibility that participatory responses may be biased and misconstrued depending on their contextual background.

The researcher believes that the information presented above together with the research questions and the lack of interpretive research on this topic makes an interpretive approach a logical choice; one that will not only provide an in-depth understanding of key stakeholder views, but also provide insight as to how the contextual and social aspects of the key stakeholders relate to these views.

3.4 Research Method

The ability of qualitative research to assist researchers in the understanding of phenomena (the views on cloud information security) by focussing on the perspective of research participants (interview and online survey participants) has made it an ideal research method to use for this study [32]. More importantly, according to Elliot, Fischer and Rennie [32] qualitative researchers understand that their own perspectives on the research cannot be ignored. Thus, allowing it to conform to this study's epistemological assumptions, stating that the researcher and the research participants are entwined and that their research interaction has a very real effect on the interview results.

On the other hand quantitative research, which is often conducted within a positivist research paradigm, is focussed on producing knowledge objective in nature [32]. It is often used for studying society by regarding it as a rigid structure, applying complicated means of manipulation in an effort to create a concrete *"snapshot"* of society as well as reducing the role of humans to mere elements open to the influence of a determined set of factors [61]. According to Morgan and Smircich [61] quantitative research methods often remove context from the elements under investigation in order to make precise measurements, as is the case with large scale surveys. This makes a quantitative research approach inadequate in answering the research questions of this study. This study aims to provide an in-depth understanding of the views of key stakeholders by investigating how their unique contextual and social environment influence the meanings they attach to the various information security concerns innate to cloud adoption. The study further admits that humans constantly contribute toward the creation of their social environment thus indicating that the use of quantitative methods are unsuitable for this study [61].

Having illustrated the unsuitability of a quantitative approach the researcher will be utilizing a qualitative approach, where multiple cases will be investigated. A qualitative case study approach allows a researcher to investigate aspects of a case, in line with its context, by consulting various sources of data. This facilitates investigation by not just focussing on one area, but rather on a variety of areas, enabling one to understand the various aspects under investigation [5]. Besides the researcher's philosophical assumptions and the reasons listed above, the following characteristics of qualitative case study research made it an appropriate choice for this study:

- It affords the researcher the opportunity to study key stakeholder views within their associated context [5,97] [83, page 4] even more so if,
- The key stakeholders' views and how these views relate to their associated context is not clearly delineated [5, 97].

Baxter and Jack [5] suggest that the researcher should provide a conceptual framework with which to determine the participants of the study, the description of any relationships (as dictated by experience, literature and logical conclusions) as well as being able to group the various concepts of the study. Yin [97] states that the creation of a well-defined conceptual framework may assist in avoiding the following caveats:

- No apparent structure to the write-up of the cases and
- The difficulty in writing and reading the write-up of the cases.

Such a conceptual framework is illustrated in *Figure 2.3* (see *Section 2.9*) and was constructed by revisiting the literature review in order to extract the core concepts of this study.

3.4.1 Online Survey

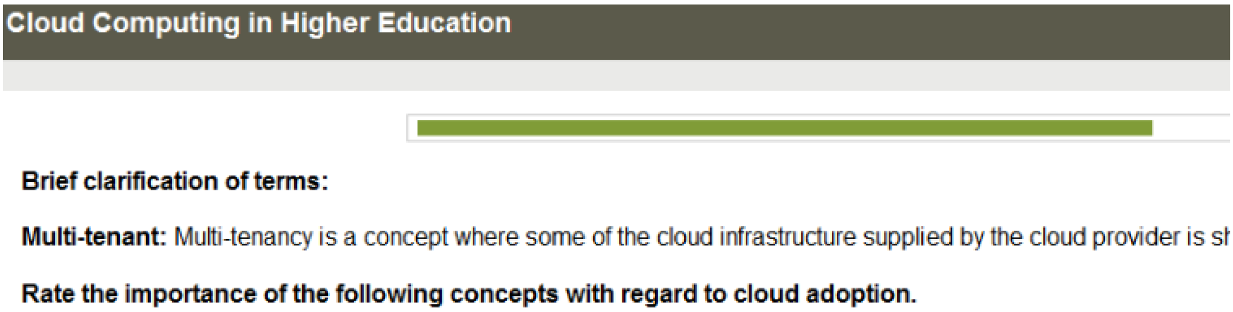
Using the aforementioned conceptual framework the researcher made use of an online survey (see *Appendix A*) to gather some preliminary data. Please note that although *Chapter Three* and *Appendix A* list the survey questions together with their purpose they do not convey the aesthetics and options each of these questions had during the actual online survey. For this reason *Appendix A* also contains a copy of the complete online survey (as it appeared to the survey respondents). The purpose of the online survey is to give the researcher some indication as to:

- The level of knowledge and experience participants (key stakeholders) have with regard to key information security concepts discussed in the literature review,
- To which extent these information security concepts affect cloud adoption from the perspective of the key stakeholder, and
- Information relating to the demographics of the participants.

The use of an online survey stems mainly from the technical nature of the core concepts present in this study. It is anticipated that such a survey would allow the researcher to gather information on a wide variety of concepts related to cloud information security, whilst keeping the results as focussed as possible. These results could then assist in pinpointing areas of particular interest that warrant further investigation. Therefore, guided by the online survey, an interview guide will be created with which to further investigate areas of interest. Using SurveyMonkey[1] the survey questions (see *Section 3.7* and *Appendix A*) will relate to the context and demographics of the participant with the rest focusing solely on information security aspects specific to cloud adoption. However, before collecting any data with the online survey it will be piloted to ensure the collection of relevant data, which could then be used in the construction of the interview guide.

Many of the design elements were intentional, such as the progress bar (see *Figure 3.1*), which informs respondents of their progress, motivating the respondents to complete the online survey [22]. This design element is illustrated in *Figure 3.1.* Related questions are to be grouped and presented to the respondent on a single page, reducing the time taken to complete the survey.Survey options are to be sorted alphabetically to avoid any bias [85] in addition to keeping the opening questions as simple as possible, which assists in building respondent confidence. Clear instructions on how to complete the survey, as well as navigational directions, are to be given at the beginning of the survey [85]. Sensitive questions relating to demographics will be inserted towards the end of the survey [85].

[1] www.surveymonkey.com



Cloud Computing in Higher Education

Brief clarification of terms:

Multi-tenant: Multi-tenancy is a concept where some of the cloud infrastructure supplied by the cloud provider is s

Rate the importance of the following concepts with regard to cloud adoption.

Figure 3.1: Depiction of progress bar in online survey

Besides these design elements the researcher will be entering all the survey participants, who have successfully completed the survey, into a draw for a small prize in the hope that it will have a positive effect on the response rate, as suggested by Heerwegh [45]. The researcher is aware that this may introduce bias into the survey results.

3.4.2 In-Depth Interviews

In order to gain a deeper level of understanding regarding these areas of interest, the researcher will be making use of in-depth interviews. Not only will these interviews allow the researcher to investigate the areas of interest, but more importantly, also the data that is socially constructed during the interviews. According to Myers and Newman [62] the qualitative interview is the most important, prevalent and powerful research instrument in qualitative research; one which can be defined as a means of acquiring an understanding with regard to,

> *"... the experiences, concerns, interests, beliefs, values, knowledge and ways of seeing, thinking and acting of the other." [78, page 10]*

For this reason semi-structured in-depth interviews are to be employed, motivated by three factors namely, (1) the researcher initiated the study with a clear idea of what needed to be researched; (2) because of this there is a need to focus on the specifics of this topic (using specific questions) and (3) this study consists of multiple universities (cases) [11, page 472]. However, only after the interview guide has been piloted will it be used in the collection of primary data. Both the pilot and post-pilot interview guide (see *Section 3.6.1*) will consist of voice recorded open-ended questions. According to Simons [83, page 52] voice recordings:

- Provide rigour in the way the interview will be portrayed and enhances its authenticity,
- Allows the researcher to fully interact with the interview participant negating the need to constantly write notes, and

- Affords the researcher the opportunity to compare any notes taken during the interview with the actual voice recording as a means of ensuring the integrity of primary data.

It is with the research instruments of these two methods that the researcher will gather data from the sources of this study.

3.5 Sources of Data

This study will collect data from multiple sources, which Baxter and Jack [5] associate with an increase in the integrity of the collected data. It is important to note that the data collected by the online survey does not constitute a direct part of the primary data, but will merely be used in the construction of a relevant interview guide. This *"mixed"* approach is motivated by the following statement:

> *"Unique in comparison to other qualitative approaches, within case study research, investigators can collect and integrate quantitative survey data, which facilitates reaching a holistic understanding of the phenomenon being studied." [5, page 554]*

The authors further state that combining data collection approaches in this way not only deepens the understanding gained, but also justifies the results that emerge from the analysis of the primary data. Driven by the research questions [11, page 422] a criterion-based purposive sampling approach will be used. For this reason the views of key stakeholders from three South African universities will be investigated. Participants from these South African universities will be selected with the criteria that they form part of senior IT management or administration.

For this reason participants occupying the following positions were selected for both the online survey and in-depth interviews:

- IT Directors,
- Systems Managers,
- IT Managers,
- Operations Managers, and
- System Administrators

Table 3.1: List of South African universities.

Name of University	Province	Web address
Rhodes University	Eastern Cape	www.ru.ac.za
University of Fort Hare	Eastern Cape	www.ufh.ac.za
Walter Sisulu University	Eastern Cape	www.wsu.ac.za
Nelson Mandela Metropolitan University	Eastern Cape	www.nmmu.ac.za
University of Cape Town	Western Cape	www.uct.ac.za
University of Stellenbosch	Western Cape	www.sun.ac.za
University of the Western Cape	Western Cape	www.uwc.ac.za
Cape Peninsula University of Technology	Western Cape	www.cput.ac.za
University of the Free State	Free State	www.ufs.ac.za
Central University of Technology	Free State	www.cut.ac.za
University of Kwa-Zulu Natal	Kwa-Zulu Natal	www.ukzn.ac.za
University of Zululand	Kwa-Zulu Natal	www.uzulu.ac.za
Durban University of Technology	Kwa-Zulu Natal	www.dut.ac.za
Mangosutho University of Technology	Kwa-Zulu Natal	www.mut.ac.za
University of Pretoria	Gauteng	www.up.ac.za
University of Witwatersrand	Gauteng	www.wits.ac.za
University of Johannesburg	Gauteng	www.uj.ac.za
Tshwane University of Technology	Gauteng	www.tut.ac.za
Vaal University of Technology	Gauteng	www.vut.ac.za
University of Venda	Limpopo	www.univen.ac.za
University of Limpopo	Limpopo	www.ul.ac.za
North-West University	North-West Province	www.nwu.ac.za

Although not strictly part of senior IT management, system administrators are to be included due to the technical knowledge they posses and the fact they often serve as an interface between the technical team and senior IT management; making them a valuable source of information. As for the variety of the survey and interview participants, Bryman [11, page 418] states that sampling with the intent to include a variety of participants is recommended when using a purposive sampling approach. This ensures that the sample members differ from each other in terms of the key concepts to be investigated by the research questions. Simons [83, page 34] states that purposive sampling often aids in the understanding of the cases under investigation. Ultimately the primary goal of purposeful sampling within this study is to ensure that participants are sampled from whom the researcher may elicit accurate and relevant information; information that will ultimately allow the researcher to address the research questions.

For the online survey the researcher will be contacting at least one key stakeholder within each of the universities listed in *Table 3.1*. In some instances more than one key stakeholder from a particular university were invited to take part in the online survey. Respondents occupying positions as listed above were chosen specifically because they form the core of what this study refers to as key stakeholders. This stems from the fact that they would regularly interface with members of senior management in other functional areas of their university as well as within their own IT department. The small sample size is motivated by the fact that:

- The researcher only has a limited amount of key stakeholders to contact,
- Purposive sampling will be employed, which will further limit the amount of possible respondents, and

- This is not a positivist study that typically seeks to produce generalizations about the views of key stakeholders with regard to cloud adoption.

To further investigate the identified areas of interest the researcher will conduct twelve in-depth interviews with key stakeholders from three South African universities (see *Table 4.2* for more information). The small sampling size of these interviews stems from the qualitative nature of this study which allows for the sampling of a smaller number of participants as suggested by Patton [67],

> *"...qualitative inquiry typically focuses in depth on relatively small samples, even single cases, selected purposefully" [67, page 169]*

To protect the sources of information the researcher decided to anonymise the participants which according to Simons [83, page 107]:

- Offers protection to staff members, since the name of an organization is not revealed,
- Allows participants to share more information, because they are not identifiable, and
- Assists the researcher in mitigating any responses that are unfair and/or insensitive.

In the next section the researcher will detail the procedures that are to be followed before, during and after the collection of data from the sources listed above.

3.6 Data Collection Method

The researcher initiated the data collection process by contacting each potential survey respondent by telephone, asking for their participation in the survey. This telephonic conversation afforded the researcher the opportunity to explain the purpose of the online survey. Following this an email will be sent to the key stakeholders who have indicated that they are willing to participate in the survey. Attached to this email message will be a *pdf* document containing detailed information about the survey as well as a link to the actual survey (see *Appendix B* for an illustration of this document).

Potential interview participants will initially be contacted by telephone. A telephonic approach was selected so that the researcher may explain the purpose of the interviews whilst at the same time giving the participants the choice of interview venue, date and time [83, page 47]. These details are to be confirmed one week before the interview is to take place. All the interviews will be voice recorded, although this may depend on participant consent (see *Section 3.6.1*). Interviews may vary in length with an anticipated duration of about 45 to 60 minutes. The decision not to make the interviews too long is based primarily on the fact that the researcher does not want to stretch the attention span of each participant, but also not to take up too much of their time at work.

3.6.1 Fieldwork Protocol

The purpose of the fieldwork protocol is to provide structure and coherence to the process of data collection.

Online Survey

1. The researcher will start the fieldwork process by submitting the pilot survey questions for ethical clearance.
2. Up to five researchers from the department of computer science and information systems will then be asked to complete the pilot survey.
3. The revised pilot survey questions will then be submitted as an appendix to the ethical clearance application.
4. Create a list of South African universities together with the contact details of at least one member of senior IT management from each of the universities listed in *Table 3.1*.
5. This will be followed by a phone call to each of the potential survey respondents (list created in step 4). The purpose of this phone call is to further describe the study, the purpose of the survey as well as to ascertain whether or not the key stakeholder is willing to participate in the survey.
6. A personalized email will then be sent to every willing respondent. Attached to this email message will be a two page *pdf* document containing detailed instructions concerning the online survey.
7. One week after the online survey instructions have been sent out a reminder will be emailed to the same list of respondents as in the previous step. Respondents who have not completed the survey two weeks after they have been reminded will be left out of the study.

Step six and seven will primarily be executed to ensure high levels of participation.

In-Depth Interviews

1. The results of the survey will then be analysed and used to create a pilot interview guide.
2. Before conducting these pilot interviews the researcher will append the pilot interview questions to the ethical clearance application.
3. Signed letters of informed consent (see *Appendix B* for an illustration of this letter) will be collected before conducting each pilot interview. The researcher will proceed by explaining the purpose of the interview making sure to ask each participant if they are comfortable with the fact the interview will be voice recorded.
4. Once the interview has started the researcher will clearly state that:
   - The interview participant has the right to terminate the interview at any time,
   - They have the right to indicate that they wish to state something *"off-record"*, and
   - Their identity will not be revealed in the study.
5. After addressing any issues relating to the content of the pilot interview guide the researcher will create the official interview guide.
6. Twelve potential interview participants (key stakeholders), will then be contacted by telephone asking for their participation in the interviews.
7. An email will then be sent out to those participants who have agreed to be interviewed asking them to indicate a suitable date, time and location for the interview.
8. Before each interview the participant will be asked to sign a letter of informed consent.
9. Upon completion of these interviews the researcher will proceed with the transcription process, by inserting pseudonyms instead of the real names of the interview participants, systems and universities.

3.7 Data to be Collected

As suggested by Baxter and Jack [5] a conceptual framework, such as the one illustrated at the end of *Chapter Two* (see *Figure 2.3*), will provide this study with the means to collect data relevant to the themes discussed in the literature, the contextual aspects of the various cases and the associated key stakeholder views. Also, because

Table 3.2: Core survey questions relating to cloud computing threats

#	Survey question	Purpose of question
10	Rate your level of experience with regard to the following cloud computing threats.	With this question the researcher is gauging the level of awareness and to some extent knowledge of specific cloud computing threats, which are listed in the question. It also serves as an indicator as to how technical key stakeholders are considering that they are strictly speaking part of management.
11	Rate your level of experience with regard to the following cloud computing threat mitigation techniques and technologies.	Here the researcher would like to investigate whether or not key stakeholders actually know how to mitigate the threats that their cloud infrastructures are exposed to. In some way it relates to direct technical knowledge, but can also indicate the level of communication between key stakeholders and their technical staff.
12	Please rank the following information security concerns in order of their susceptibility to cloud computing threats. A selection of 1 would indicate that the information security concern is most susceptible with a selection of 3 indicating it is least susceptible.	The purpose of this question is to make the participant choose which information security concern is most affected by cloud computing threats from their point of view. Answers to this question together with those of question nine and ten could indicate whether or not there is some consistency in the way the participant has answered the survey questions.

Table 3.3: Core survey questions relating to security incident response and cloud adoption

#	Survey question	Purpose of question
7	Rate the importance of the following concepts with regard to cloud adoption.	This is a key question which measures the views of the respondents with regard to several aspects of cloud adoption. These aspects are not all directly related to information security, but in most cases do affect it indirectly. Many of these aspects are used in the surveys mentioned in *Section 2.8* of the literature review and will form a core component of what will be covered during the interviews.
14	Please rate your level of experience with regard to the following aspects of security incident response in a cloud environment.	Again, the purpose here is to measure how much the respondents know about concepts that will come up during the interview process.

these themes are directly related to the research questions of this study the conceptual framework will provide additional focus and guidance in this regard.

The researcher also anticipates that the interpretive nature of this study will enhance the level of understanding and create additional knowledge (relationship between context and views) as a result of the interaction between the researcher and research participant [53]. From this additional knowledge the researcher would then be able to revise the initial conceptual framework as set forth in *Chapter Two*. For these reasons the researcher deems it necessary to demonstrate how the collected data (via online survey) aligns with the research questions of this study.

In the online survey data surrounding threats and security incident response is collected by the questions represented in *Table 3.2* (threats and threat mitigation) and *Table 3.3* (security incident response). These concepts are discussed in the literature review (see *Section 2.5, 2.6 and 2.7* respectively) and address the first and second research questions (see *Chapter One*). It is important to note that although cloud architecture does not directly address a research question it provides this study with important background information. Concepts relating to cloud architecture is discussed in *Section 2.2* and *Section 2.3* of the literature review with related survey questions contained in *Table A.2* of *Appendix A*.

Table 3.4: Interview question relating to all three research questions

#	Interview question	Research question addressed	Purpose of question
1	How do you view the benefits that cloud computing offers your university, taking into consideration the additional threats and potential security incidents it could expose your university to?	Main research question as well as the first and second research questions.	As discussed in the literature review (see *Section 2.4*) there are several reasons why organizations are moving towards the cloud. From *Section 2.5* one can see several reasons why many organizations have not opted to move towards the cloud. This question aims to understand how university key stakeholders view this and whether or not they agree that it can enhance the services they offer their students similar to those universities mentioned in chapter one. It enquires whether or not they deem a move towards the cloud as beneficial to their day to day running (administratively) of the university. In a survey conducted by Appirio [1] 28% of cloud adopters cite security as the biggest misconception with regard to cloud adoption, which may or may not be echoed by key stakeholders within higher education. Additionally authors such as Erenben [33] state that the use of the cloud could enhance security, thus forming part of the benefits of cloud computing.

As one of the core concepts of this study the views of key stakeholders with regard to cloud information security has purposefully not been encapsulated by cloud architecture, as illustrated in *Figure 2.3*. This stems from the fact that the literature suggests that these views are not directly dependent on the cloud architecture in use. The studies mentioned in the literature review, such as the one conducted by Appirio [1], do however indicate that key stakeholders view the security of cloud-based information differently, depending on whether or not these views are captured pre or post cloud adoption. This is illustrated towards the top right of *Figure 2.3* where the reader is able to see that key stakeholders tend to view the cloud in a negative light pre-adoption, but tend to view the cloud in a positive light post adoption. Data surrounding the adoption of cloud computing will be collected by question seven (see *Table 3.3*).

Another core concept illustrated by *Figure 2.3* is that of the context within which participants operate. This core component of an interpretive study is captured by not only collecting data pertaining to key stakeholder views, but also data specific to the context of each case. This includes how cloud computing services are used as well as the demographics of each participating university. This concept is illustrated on the right-hand side of *Figure 2.3* and is aligned with the survey questions contained in *Table A.3* (see *Appendix A*). A complete illustration of the online survey questions can be found in *Appendix A*.

It is anticipated that the initial conceptual framework, together with the survey data, will provide this study with an accurate and focussed conceptual lens, one that will allow the researcher to construct an accurate data collection instrument.

Table 3.5: Interview questions relating directly to the first research question

#	Interview question	Research question addressed	Purpose of question
2	Some individuals have described cloud computing as a security nightmare, so much so that it can't be handled in traditional ways. In your opinion, how does the openness of most university networks affect threat mitigation techniques and/or technologies within a university cloud infrastructure?	Research question one.	In *Section 2.6* of the literature review several technologies and techniques are discussed that could be used to mitigate cloud computing threats or threats to cloud enabling technologies (i.e., hypervisors). The purpose of this question is to find out if key stakeholders think threat mitigation can be applied in traditional ways, or does the cloud indeed require special treatment with regard to threat mitigation and information security in general. In essence this question investigates the participant's views on the traditional way of dealing with threats that compromise information security and whether or not this is applicable to the cloud. For example, the Ponemon Institute found that IT practitioners don't believe that their organization is capable of securing data and applications within the cloud [68]. Responses to this question might confirm that universities also fall into this category.
3	In your university what role do you think cloud computing threats play with regard to cloud information security, specifically the confidentiality, integrity and availability of information?	Research question one.	The literature review investigated several threats, some specific to the cloud. More importantly all of them lead to the compromise of the confidentiality, integrity or availability of information (see *Section 2.5*). The purpose of this question is to understand how the participant thinks about cloud computing threats and the relationship between these threats and information security. Do they agree or disagree and to which extent? Also, do participants attach as much importance to threats and the management thereof, as the participants of the study conducted by the Data Security Council of India [25]. Participants of this study listed threat management as the third most critical data security challenge in the cloud. Responses to this question might also uncover additional concerns over and above the others listed above, fostering further conversation around this core component of the study.

Table 3.6: Interview questions relating directly to the second research question

#	Interview question	Research question addressed	Purpose of question
4	How does your university currently respond to security incidents?	Research question two.	The literature review (see *Section 2.7*) discusses the various phases of the security incident response life cycle. In this review the Cloud Security Alliance [19], the SANS Institute [75] as well as Grobauer and Schreck [42] mention that both the cloud provider and customer should be in agreement as to how security incidents in the cloud should be handled and who will be responsible for which aspect of the security incident response process. The purpose here is to ascertain whether or not key stakeholders do indeed share this point of view and to what extent. It also endeavours to uncover whether or not South African universities do have security incident response plans in place. If they do, a comparisons could be made with what is suggested by the authors in the literature review. From a higher education perspective there may be additional factors to consider.

Table 3.7: Interview questions relating directly to the main research question

#	Interview question	Research question addressed	Purpose of question
5	How do you think the transparency of cloud provider operations would influence the cloud adoption process within your university?	Main research question and indirectly the first and second research questions.	In the literature Monfared [60] states that many cloud providers still believe that the best form of defence is to obfuscate their internal cloud operations. On the other hand Wrenn [94] states (see *Section 2.5*) that cloud providers should be more transparent with their customers. The purpose of this question is to understand whether or not participants from institutions of higher education view and perceive cloud provider transparency as a good method for accelerating cloud adoption or not. This question is also aimed at probing their views on the adoption process (hence relevance to main research question), but it is equally applicable to security incident response as well as threats and threat mitigation. In essence this question sets out to investigate whether or not transparency in terms of threat mitigation, threats (realised or unrealised), breaches and security incident responses are of concern to universities and how it ultimately affects the adoption process itself.
6	In your opinion, what are the major cloud adoption stumbling blocks in your institution?	Main research question	The literature review contains many authors who primarily cite security as one of the top adoption stumbling blocks. This is confirmed by surveys that were conducted by Appirio [1], PriceWaterhouseCoopers [69], the Data Security Council of India [25] and The Ponemon Institute [68] (see *Section 2.8*). This question aims to find out if the participant agrees with these findings and statements or are there other more prominent adoption stumbling blocks from a higher education perspective. Responses to this question might also afford the researcher the opportunity to obtain a deep understanding of all the concerns that affect adoption within South African universities.

3.7.1 Data Collection Instrument

Since this study relies on in-depth interviews for the collection of primary data, it follows that the data collection instrument be an interview guide. This interview guide contains open-ended questions that have been specifically chosen to foster conversation around the concepts central to this study. From the questions listed in *Table 3.4, 3.5, 3.6* and *3.7*, it is evident that only questions directly related to research questions have been included in the interview guide. Each of these questions cover a theme with the intention that it becomes a point for further discussion rather than just a question with a corresponding answer.

Great care has been taken to ensure that each of the six interview questions will afford the researcher the opportunity to ask relevant follow-up questions. This will provide further depth to the concepts that indirectly and directly affect the concepts contained in that specific interview question. In addition to the structure and format of the questions careful consideration has been given to the order in which these questions appear on the interview guide, ensuring that questions of a less threatening nature appear towards the start of the interview. This will aid in building rapport with the interviewee so that he or she may feel comfortable during the interview [28].

The researcher has also ensured that all of the interview questions are structured in such a way that they address the specific views of the interview participant in relation to their own university. This enables the interview guide to capture responses that are not general, but rather quite specific allowing for the elicitation of contextualized responses.

3.8 Data Treatment

To analyse the primary data the researcher will be employing thematic analysis. Although many studies make use of the principles that underpin thematic analysis, most do not explicitly state its use [10]. At its core thematic analysis is,

> *"... a method for identifying, analysing and reporting patterns (themes) within data." [10, page 79]*

As a method of analysis it is not only suited to a wide variety of interpretive research designs, but is also a useful method of analysis for novice researchers [53]. In addition to the aforementioned advantages, thematic analysis can also be applied in an inductive or deductive manner. However, the fact that it relies heavily on transcribed data makes it vulnerable in terms of the transcriptions' quality. Its interpretative nature also limits the generalizability of its results.

In accordance with Braun and Clarke [10] the data is analysed in a process spanning six phases. During the execution of phase one, Braun and Clarke suggest that the researcher become acquainted with the data that has been collected. One option is to personally transcribe the interview data, which could assist in the process of creating meaning and overall understanding. In this study the researcher will not only personally transcribe all of the in-depth interviews, but also re-read those transcripts during the process of analysis. The researcher would also like to point out that the transcription process will form part of the preliminary interpretation and analysis of the raw primary data (voice recordings of the in-depth interviews) [7]. Although this process is usually taken as a mere requirement in order to perform the latter detailed analysis, the nature of the main research question demands more than just transcribing the actual words of the interviews. For this reason careful attention will be given to the accuracy of the transcriptions. This will ensure that it retains its original integrity, especially when it comes to punctuation, non-verbal gestures and other contextual indicators such as the tone used by the participants. All of the latter components are to assist the researcher in the interpretation of the primary data.

Initial codes pertaining to the *"interesting aspects"* of the primary data are to be created during the execution of phase two. However, before this can be done a clear definition of what constitutes *"an interesting aspect"* should be formulated. This process of deduction will, for the most part, be guided by the research questions of this study, assisting in the eventual creation of a coding framework [3]. During the execution of phase two this coding framework will contain a list of codes and the data extract/s relating to that code. To enrich the analysis process, Braun and Clarke [10] encourage researchers to code as many data extracts as is relevant. This may lead to instances where a data extract has been coded multiple times or where a particular code is associated with more than one data extract [10]. Although Braun and Clarke [10] state that the coding process be either theory (deductive) or data (inductive) driven, it is anticipated that phase two's coding process will be more theory driven and will span the entire data corpus. Phase two will culminate with the creation of a coding framework containing a list of codes and the collated data extracts with which it is associated.

Only during the execution of phase three will the researcher start identifying candidate themes from the codes that have been identified in phase two. At this point the researcher has the choice of identifying either latent or semantic themes. Due to the interpretive nature of this study the focus will be on identifying latent themes, which would assist the interpretive process. It is important to note that at this stage Braun and Clarke [10] suggest that no candidate themes be eliminated, since even themes which appear to be irrelevant may very well be merged with other themes; especially during phase four. Phase three culminates in not only the expansion of the coding framework, which now contains a list of themes, associated codes and all the data extracts that have been collated under these codes (phase two), but also an initial thematic map.

Phase four will be mostly concerned with the refinement of the candidate themes identified during the execution of phase three. This process is characterised by either identifying new themes, merging themes or eliminating themes all together. The end of phase four will result in a final coding framework spanning the entire data corpus. This will be followed by a process of further refinement (phase five), differing from the previous phase in the sense that the themes will now be defined by providing a persistent narration created from all of the collated data extracts within each theme (as contained in the coding framework); illustrating interpretive rigour [38]. The final thematic map will form the major deliverable of phase five. Lastly, phase six will be concerned with the detailed analysis of each theme within the framework of the final thematic map created at the end of phase five.

3.9 Summary

In this chapter the researcher illustrates all the elements which form a central part of this interpretive research design. Specific reference is made to the research methods, paradigm and data analysis. The online survey questions, interview guide and conceptual framework are probably the most important elements, since they address the research questions of this study. In the following chapter the results of the online survey as well as the in-depth interviews are discussed.

Chapter 4

Analysis and Interpretation

4.1 Introduction

Chapter Three gave the reader an indication of how the researcher will collect and analyse the survey and interview data. The reader was presented with a set of survey and interview questions (see *Section 3.7* and *Appendix A*) as well as the procedures to follow during the data collection process (see *Section 3.6.1*).

In this chapter the reader will be presented with a brief overview of the survey results, making specific reference to how it influenced the creation of the interview guide. The organizational context of each university will be revisited in *Section 4.3.1* followed by a practical outline of the processes that constituted the thematic analysis of the interview data (*Section 4.3.2*). This will be followed by a detailed analysis and interpretation of the identified themes, making specific reference to the conceptual frameworks aligned with each main theme (see *Section 4.4*.

4.2 Online Survey

Following the fieldwork protocol (see *Section 3.6.1*) the researcher contacted at least one key stakeholder within each of the universities listed in *Table 3.1*. In all, 33 key stakeholders were invited to complete the online survey. From this 11 responded, resulting in a 33% response rate (see *Table 4.1*). A complete listing of the online survey questions can be found in *Appendix A*.

The exploratory and anonymous nature of the online survey does not afford the researcher the opportunity to understand exactly how specific universities responded.

Table 4.1: Online survey responses

Total survey invitations	33
Total survey responses	14
Incomplete survey responses	3
Usable survey responses	11
Survey response rate	**33%**

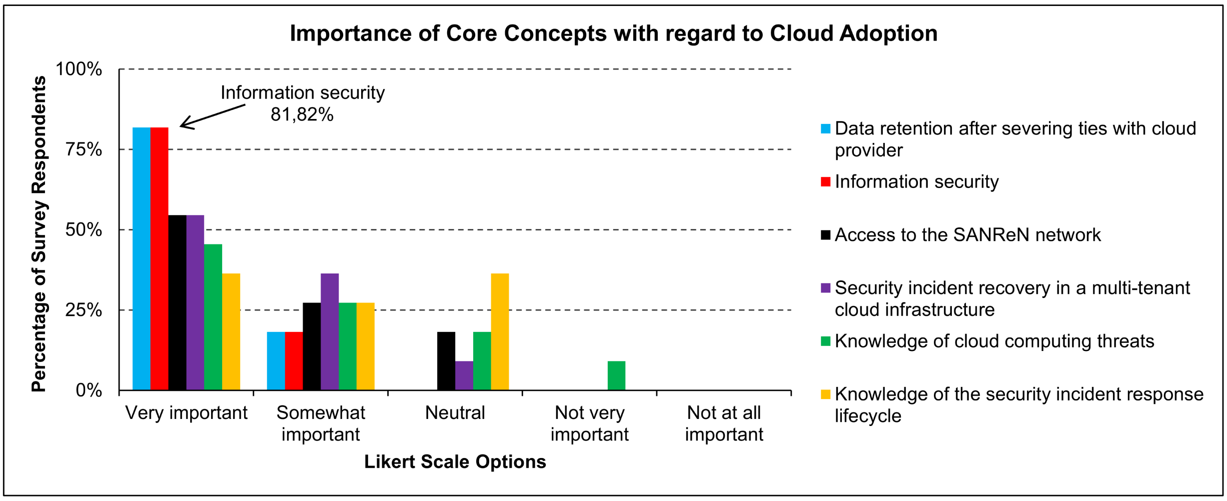


Figure 4.1: Importance of core cloud adoption concepts

4.2.1 Cloud Adoption

In the seventh survey question, respondents were asked to rate the importance of certain concepts with regard to the adoption of cloud computing (see *Table 3.3*). Respondents had to indicate their level of agreement on a five point Likert scale ranging from *"Not at all important"* to *"Very important"*. After analysis of the survey results relating to the fourteen cloud adoption concepts the researcher created a graph illustrating the *"core"* concepts of this study (see *Figure 4.1*).

Figure 4.1 gives some indication that information security is viewed as a very important concept when considering a move towards the cloud, with over 81.82% of respondents rating it as *"Very important"*. The graph also illustrates that respondents' views are fairly divided when it comes to knowledge pertaining to the security incident response life cycle. This is interesting, especially if one considers that 54.55% of respondents rated *"Security incident recovery in a multi-tenant cloud infrastructure"* as *"Very important"* whilst 36.36% od respondents rated *"Knowledge of the security incident response life cycle"* as *"Very important"*. This might be an indication that key stakeholders expect the cloud provider to take responsibility for responding to security incidents, since this would require extensive knowledge of the security incident response life cycle. The fact that *"Security incident recovery in a multi-tenant cloud infrastructure"* is ranked so high could also be an indication that key stakeholders view

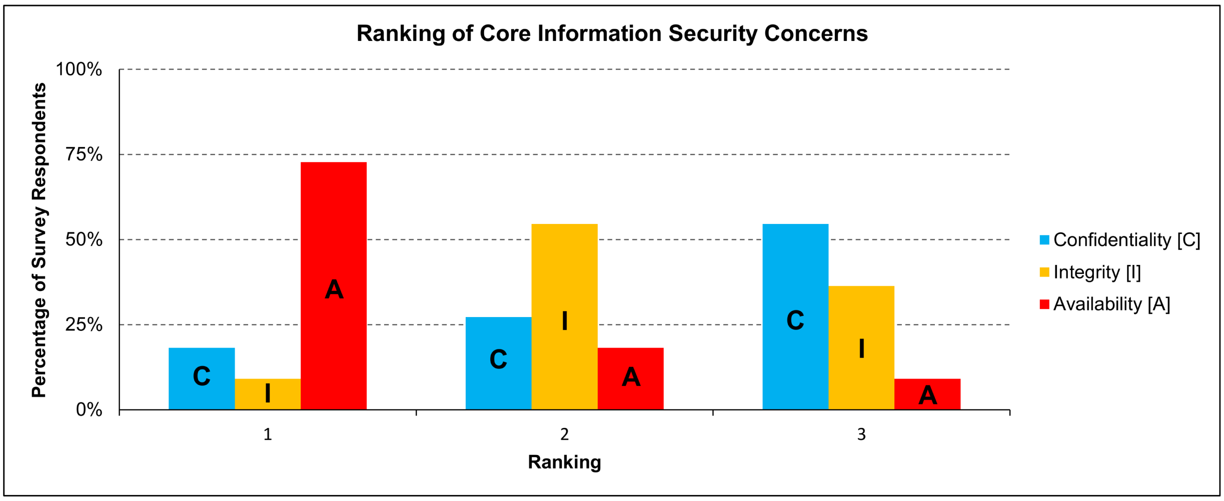


Figure 4.2: Ranking of core information security concerns

the cloud as a turn-key solution.

Correlation between the interview guide and *Figure 4.1* can be found by inspecting interview question one, and interview questions three to six (see *Section 3.7.1*).

4.2.2 Information Security

Question twelve (see *Table 3.2*) of the online survey asked respondents to rank the three core information security concerns in order of their susceptibility to cloud computing threats. From *Figure 4.2* the reader is able to see that many of the respondents believe that availability is most susceptible to cloud computing threats. To some extent this corresponds with the importance given to the concept *"Access to the SANReN network"* as well as *"Information security"*, as illustrated in *Figure 4.1*. It is worth mentioning that although availability was ranked as the most susceptible to cloud computing threats, over 75% of respondents regard *"Data retention after severing ties with cloud provider"* as a *"Very important"* adoption concept, which indicates that confidentiality also plays a large role when considering a move towards the cloud. In fact, this concept was the highest rated together with *"Information security"* (see *Figure 4.1*).

Interview question three investigates how the participants view all the core information security concerns in relation to cloud computing threats as well as any knowledge gaps of which the researcher may be unaware.

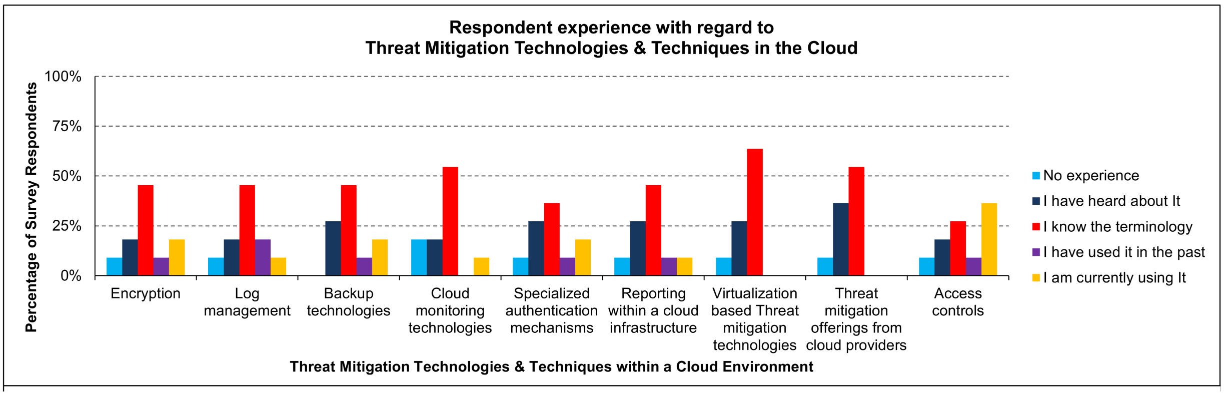


Figure 4.3: Threat mitigation experience in the cloud

4.2.3 Threats and Security Incident Response in the Cloud

In *Figure 4.3* the level of experience respondents have with certain cloud computing threat mitigation technologies and techniques is illustrated. The second interview question seeks to accomplish this in an indirect manner by investigating whether or not the interview participants view traditional threat mitigation as a valid means of dealing with cloud-based threats. This in turn requires knowledge and experience of threat mitigation technologies and techniques. It is worth noting that although 54.54% of the respondents stated that their universities officially use cloud computing, many key mitigation techniques and technologies are not well known and in some instances not even used. This might be an indication that key stakeholders either:

- Assume that the cloud provider has implemented some or all of the mitigating technologies and techniques listed in *Figure 4.3*;
- Have not engaged with their cloud providers about whether or not these technologies and techniques are used indicating a lack of communication between the cloud provider and the cloud subscriber (university); or
- In the event of a private cloud, key stakeholders are not communicating effectively with the relevant technical stakeholders as to what is or should be used to mitigate cloud computing threats.

It is of course also possible that in some instances all three of the above statements are applicable. One also has to bear in mind the fact that some universities might not officially be making use of cloud services, which might also explain the data as illustrated in *Figure 4.3*.

When asked to indicate their level of experience with regard to security incident response (question fourteen in online survey) several respondents indicated that they had no experience with most of the concepts contained in

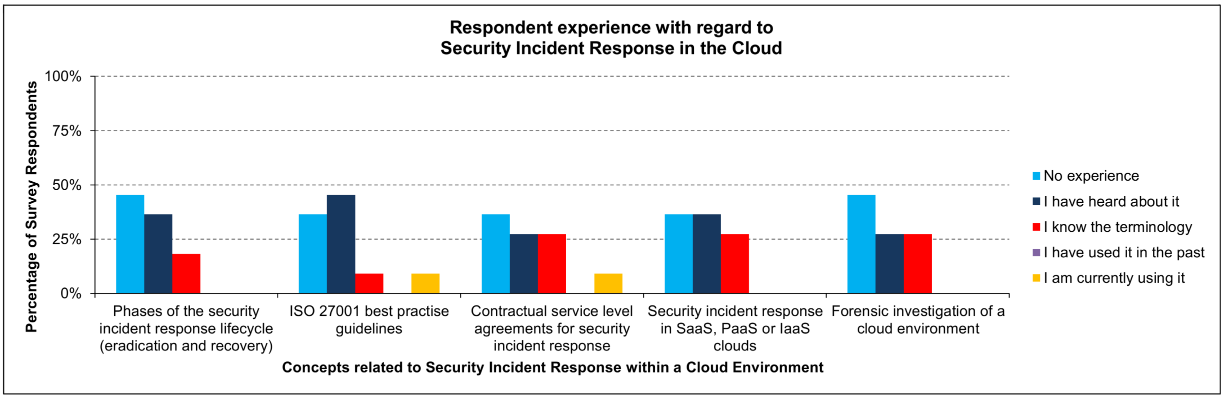


Figure 4.4: Security incident response experience in the cloud

this question. Although more than half of the respondents indicated that they were officially making use of cloud computing, very few indicated that they were making use of explicit service level agreements. This is interesting, since Grobauer and Schreck [42] indicate that service level agreements are a useful method of establishing what each party is responsible for when reacting to security incidents (for more detail see *Section 2.7*). Interpretation of *Figure 4.4* may indicate that:

- Cloud subscribers expect their cloud providers to take responsibility for security incident response in the cloud, hence the lack of experience with regard to the concepts illustrated in *Figure 4.4* or
- Universities are making use of a cloud computing model where they feel that there is no need to develop and apply formal security incident response plans (possibly private or community cloud).

The results shown in both *Figure 4.3* and *Figure 4.4* may also indicate that cloud computing is still within a phase of adoption where it is being evaluated, hence the relatively low levels of experience with regard to threat mitigation and security incident response. Using the information presented in these graphs aided the researcher in the creation of interview question four and five (see *Tables 3.6 and 3.7*). It is anticipated that these questions would not only elicit direct responses, but also highlight the contextual differences leading to these varying levels of experience.

4.2.4 Summary of Online Survey

Although the results of the online survey have been illustrated using graphs and some suggestions have been given as to how this information may be interpreted, it is recognised to be by no means statistically significant, because of the small number of respondents. For this reason the researcher did not investigate the relationship between these concepts. However, without even considering these relationships, the following important themes emerged:

- Information security is indeed a concern when looking at the adopting of cloud computing.
- Key stakeholders may expect their cloud providers to have more responsibilities with regard to threat mitigation and security incident response in the cloud, and
- That availability plays a big role when considering a move towards cloud computing.

It was during the interview process that these themes, together with the concepts obtained from the literature (see *Section 2.9* in *Chapter Two*), were further explored.

Table 4.2: Interview details per University

University pseudonym	# of Participants	Participant pseudonyms	Purpose
University A	5	A,B,C,D,E	Research intensive
University B	5	F,G,H,J,Z	Comprehensive
University C	2	L,M	Research intensive

4.3 In-Depth Interviews

As stated in *Chapter Three* twelve in-depth interviews were conducted with participants from three South African universities (see *Table 4.2*). These universities vary in size as well as the variety and type of education they offer.

4.3.1 Contextual Background

University A

As one of the smaller research intensive universities in South Africa, participants from University A expressed some very mature thoughts on cloud security and incident response. Using the cloud for more than just one system made their views even more compelling. Most of the participants involved in the process of actually adopting the cloud had very clear and well defined ideas on what is required to make their cloud implementations safe and secure; not to mention operationally feasible.

With University A still evaluating some components of their public cloud solution, adoption has only been partially completed. From the interview data some of the reasons for this include:

- Information policy with regard to information hosted in the cloud,
- Emergency access to institutional information in the cloud, and
- To a lesser degree, availability and resiliency of Internet connectivity.

This does not preclude the existence of some very unique views on the security of cloud-based information as well as security incident response. More often than not the researcher was able to equate these differences to the varying operational contexts of each participant during the interview process.

From the interviews it was also clear that SANReN will have an effect on the future of cloud adoption within this university, but that it was too soon to get an indication as to what exactly this effect will be; mostly due to the fact that they have only recently attained a high speed connection to SANReN.

Many participants did not view the university's location to make any substantial difference to cloud security or adoption, especially with the arrival of SANReN. Early on during the interview process it also became apparent to the researcher that this maturity was the result of not only meticulous planning, but also the fact that University A is a cloud provider; not only to its own staff and students, but also to other universities in its region.

University B

With one of the larger user populations spread across six geographically dispersed campuses, University B has been officially making use of public cloud computing for quite some time. This together with the fact that they employ a dedicated information security officer makes for some interesting views on cloud information security. Regardless of any security concerns that may have existed, they still decided to go ahead and adopt the cloud; albeit for a subset of their user population. This seemed to have been a financial decision, since the sheer cost of providing the same features as the cloud provider would have been too great, as stated by Participant G:

> *"Now obviously the benefits outweigh the security concerns at the time we went over, because the infrastructure cost to house the students [email] at that point in time I think really outweighed security concerns. . . "*

However, from the interview data it is clear that they do not intend to adopt the cloud wholesale, especially not for core university systems. This, together with the fact that they are already using the cloud, makes this a very interesting point of view. From the data collected reasons for this include:

- Prioritization of university data in accordance with its relative importance,
- Mistrust of cloud providers,
- Issues relating to local versus international bandwidth,
- Importance of the physical location of cloud-based data, and
- Experiential knowledge gained from their current cloud computing solution.

It is also interesting to note that although they are cloud subscribers to a system provided by University A, none of the participants viewed it as such alluding to the fact that their definition of a cloud differs from the participants at University A. Unlike University A, University B is classified as a comprehensive university by CHET [14]. It has also been connected to SANReN for quite some time with many of the participants viewing a high speed Internet connection as a major cloud enabler [77]; one without which they would probably not have adopted their current cloud solution.

University C

University C has a substantial number of staff and students spread across four campuses. University C also offers a very wide range of graduate and post graduate programs. The relevant key stakeholders at University C have decided to evaluate the cloud carefully, which is exactly what they are doing presently. The fact that the interview participants listed such a wide variety of cloud adoption stumbling blocks indicates that they have thoroughly assessed the cloud. These adoption stumbling blocks include:

- Concerns surrounding continued access to institutional information hosted in the cloud,
- Uncertainty around the financial implications of using the cloud,
- Job security for IT staff,
- Quality of access to cloud-based information, and
- An IT department which feels the need to provide all the university's required services in-house

Connectivity to SANReN is seen as a positive driving force towards cloud adoption with a strong belief that South African universities should work together. Participants hinted that such collaborative work could include participating in a community cloud built specifically for South African universities. As far as the major proponents of cloud adoption is concerned University C's participants had very diverse answers, which might indicate that there is more than one group of users evaluating cloud computing as a whole.

4.3.2 Process of Analysis

All of the in-depth interviews were analysed together (forming one data corpus) using the methods outlined by Braun and Clarke [10]. Of all the themes identified by this process only those containing concepts central to this study were subjected to further interpretation; resulting in the creation of a cross-case narrative centred around these themes. It is vital to note that although Braun and Clarke make a clear distinction between theory and data driven analysis the researcher found that the quality of analysis increased quite substantially when these two approaches were used in a complimentary fashion, as suggested by Fereday and Muir-Cochrane [38] as well as the collective works of Schutz [79–81]. Braun and Clarke [10] also specifically mention that,

> *"... data are not coded in an epistemological vacuum." [10, page 84]*

This became even more evident after transcribing and reading through the first few interviews. For this reason the researcher decided to employ a more data driven approach, at least during the initial phases of analysis. After the identification of any relevant themes from the raw data the researcher was then able to relate this back to the theory obtained in the literature. This hermeneutic cycle [21, 53] was repeated several times across all six phases of analysis (as detailed in *Section 3.8*). The researcher has provided details surrounding the mechanisms that constituted the actual process of analysis below. These mechanisms are described in the context of all six phases with a strong focus on the identification of latent as opposed to semantic themes.

Phase One: Great care was taken in the transcription of all the interviews. As stated in *Chapter Three* this phase was seen as an important part of the analysis process, since it not only formed the foundation of all the analysis work which followed, but also because it afforded the researcher the opportunity to become embedded in the data. Having transcribed all the interviews further aided this familiarization process. It is during this phase that the researcher made an initial list of relevant concepts that may form part of any possible themes. This in turn assisted in the execution of phase two, since at least some initial analysis had been performed.

Phase Two: Execution of phase two required coding the entire data corpus, which resulted in a coding framework containing information beyond the core concepts of this study. This process involved analysing each interview transcript bearing in mind the list that was created in phase one. Initial coding was more data than theory driven so as not to miss any information that might have been of interest later, which involved creating codes for specific data extracts. According to the mechanisms that constitute phase two, data extracts may be coded multiple times. This is illustrated with examples in *Table 4.3* where column two contains multiple codes

Table 4.3: Data extracts that have been coded multiple times

Data extract	Code	Line in transcript
The major thing as far as our lot is concerned is connectivity and that's the thing we suffer from the most. Getting disconnected. And that's kind of foremost in our minds about if were not connected then we can't work we'd rather have it here and when the connection does go down at least we can get on with what we are doing.	• Concerned about connectivity to cloud • Prefers data to be hosted locally	114-119
A lot of people see cloud as something they don't use. I would not even just talk about the security threats etc... but take it from the most basic. Lets understand cloud computing then work through the security issues etc... I think there is a lot of hype. Unnecessary hype in terms of the security. I think we are so many other things we are making a mountain out of a mole hill.	• Understanding cloud first then security • Cloud security surrounded in hype	521-527
Yes and the reason being I want to know, because it firstly would be a test in terms of how they react to things. The fact that it didn't affect me would be a good sign. So it's part of understanding how they react in terms of when they're at risk. Secondly if there's consistent breach I would possibly want to change my service provider.	• Cloud providers should disclose • Insight into their incident response practises • Constant breach prompts change	636-641

for the data extract it is associated with (in column one). The third column in *Table 4.3* allows for easy navigation of each participants' transcript.

Some of the codes could also be associated with more than one data extract. This type of coding is illustrated in *Table 4.4* where the first row contains an example of three data extracts that are associated with one code (in column two). During the execution of phase two the researcher was cautious not to interpret the data extracts, but to rather create a coding framework based on that which was actually said.

Phase Three: In phase three the researcher identified candidate themes and any associated sub-themes from the coded data extracts. An extract of one such candidate theme (and sub-themes) is given in *Table 4.5*. The reader will notice that each code (in column three) has an alphabetic character associated with it. This not only identified the participant where the code originates from, but also aided further analysis. Using this form of data organization became especially useful during phase four where the candidate themes had to be refined and their associated data extracts collated. Care was taken not to eliminate any themes at this stage, but to rather form as many candidate themes as possible.

Phase Four: Phase four consisted of a dual process whereby the candidate themes were refined on two levels. Firstly, the collated data extracts had to undergo scrutiny as to whether or not they tied into the candidate themes with which they were associated. Once complete, evaluating the themes across the entire data set occurred. This ensured that the identified themes were valid in relation to the data set as a whole and that it captured the

Table 4.4: Data extracts classified under the same code

Data extract	Code	Line in transcript
• The availability of Internet bandwidth is of major concern. • . . . the only concern that has ever been raised is what happens when the Internet goes down, which astounds me. • . . . the availability of Internet bandwidth was a big thing. It has not fallen off the radar.	Availability concerns	37,211-212,858-859
• . . . combine your knowledge combine your skills combine your understanding and then come with recommendation[s]. Whereas [an] individual institution you might feel isolated you might be scared even financially is it the right way to go. • Why do you have recreate, at each institution re-establish, redevelop you know why do you have to have your skill. . . you can't have one institution have the complete skill set to serve all the needs on campus. We know that's the truth. So what do we do? Rather combine those strengths.	Advantages in community cloud	171-175,218-221

Table 4.5: Extract from a candidate theme

Candidate theme	Sub-themes	Code
Knowledge of cloud security	• Mitigation in the cloud • Threats in the cloud • Cloud security awareness	• Knowledge of contract with cloud provider [E] • First understanding the cloud then security [A] • Knowledge of mitigation from experience [D]

Table 4.6: Refined theme together with some collated data extracts

Refined theme	Data extracts
Security by Assumption	• For instance it's reasonably easy to assume that [Provider A] takes security fairly seriously. [E] • . . . between [System B] and [University A] is a stipulation that they do two backups. So yes those backups are run and they are then. . . I think one is on campus and I think the other one is off campus. I'm not sure, but I trust them. [A] • You have to be transparent, because people assume all sorts of amazing things of what's going on. So unless you're upfront of what you do and what you don't, particularly what you don't do. People assume their data is always backed up and you have to [be] upfront. . . [D] • I wasn't part of that evaluation process; obviously security must have been. [L] • I think fair use and abuse and those sort of things are highlighted or the understanding is that [Provider F] endeavours, because they [are] offering a service, they endeavour to do everything in their power you know to make sure that that's not being abused or open. [G]

meanings as they were portrayed by the participants. This two-step process resulted in some themes being eliminated, renamed or merged with other candidate themes. An extract of one such theme, together with the data extracts collated under its name, is illustrated in *Table 4.6*.

Phase Five: After reading the entire interview data corpus the researcher used the output of phase four (refined themes) to construct the final thematic map (see *Figure 4.5*). As suggested by Braun and Clarke [10] these themes were organized so that they do not overlap, which is illustrated by the fact that there is no association between the two main themes (*"Trust in Cloud"* and *"Views as Subscribers"*). As the primary output of phase five, it was the final thematic map which enabled the researcher to interpret the data extracts associated with these themes.

Phase Six: Phase six concluded the process of analysis resulting in the creation of a narrative based on the researcher's interpretations of:

- The identified themes and the data extracts associated with them,
- The context within which these data extracts were embedded, as well as
- Each university's operational and security context.

Throughout this narrative the researcher highlighted the contextual differences between the participating universities. This involved not only providing the reader with participatory statements to support these arguments, but also interpretations of the relationship between these statements and operational context of these participants and universities. Where applicable references to the literature were made and thus also formed part of the interpretations made within that context. In the following section the reader is presented with the resultant narrative, wherein all the main and sub-themes are discussed.

4.4 Thematic Interpretation

During further analysis of the illustrated themes, several related concepts emerged. From this the researcher decided to create two new conceptual frameworks. One for each of the main themes illustrated in the final thematic map (see *Figure 4.5*). Used in combination, these new conceptual frameworks and the final thematic map guided the interpretation process. To better illustrate these new frameworks the researcher decided to

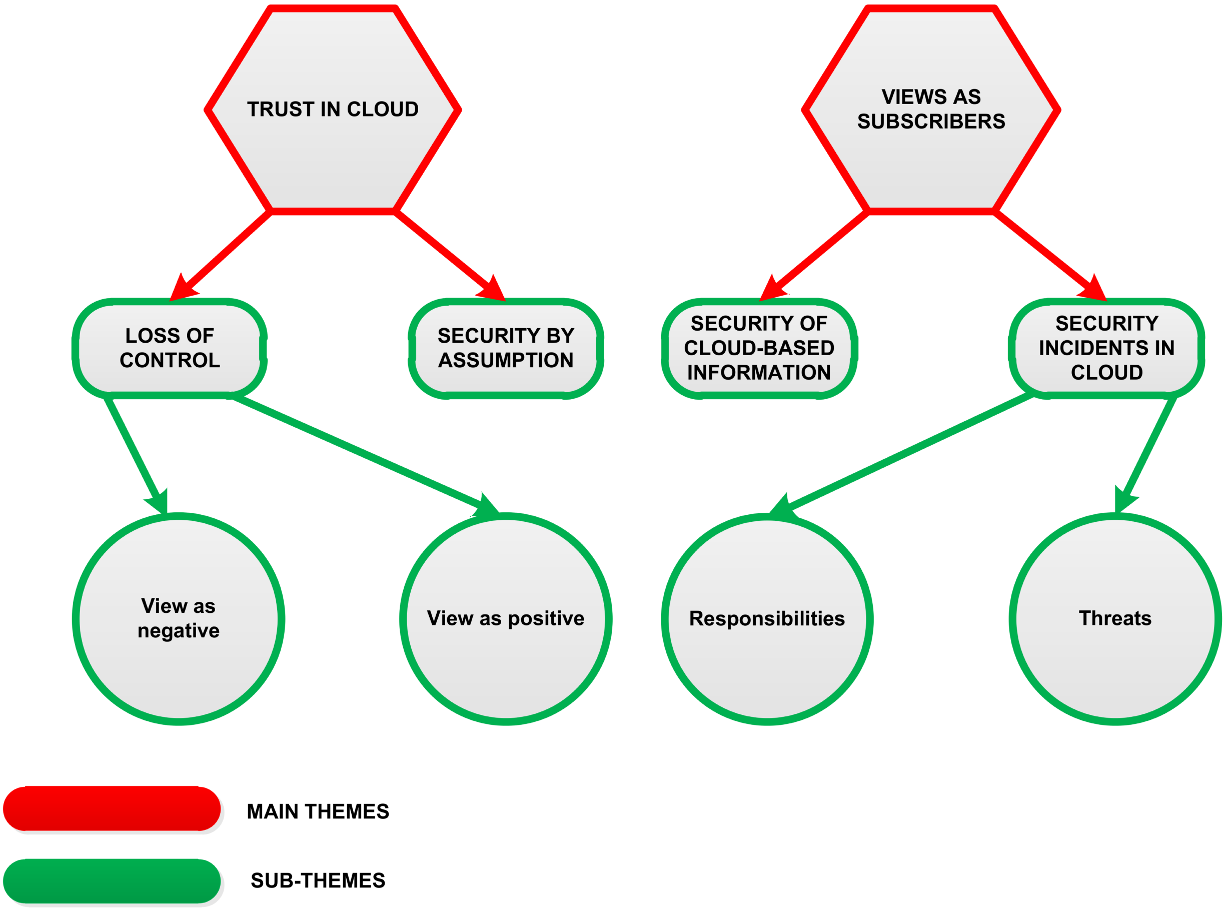


Figure 4.5: Final thematic map

provide the reader with the conceptual framework before interpreting the main theme with which it is associated (see *Figure 4.6* and *Figure 4.7*). It is anticipated that this will not only assist the reader in understanding how the concepts are related, but more importantly why they are related.

4.4.1 Trust in the Cloud

The data driven nature of this main theme resulted in few references being made to the literature during the interpretation of data related to this theme. This is amplified by the fact that although the term *"Trust"* was not directly used in any of the interview questions it emerged as a central theme from the interpreted data. It is for this reason that it has been depicted as a main theme (see *Figure 4.5*) and a core concept in *Figure 4.6*.

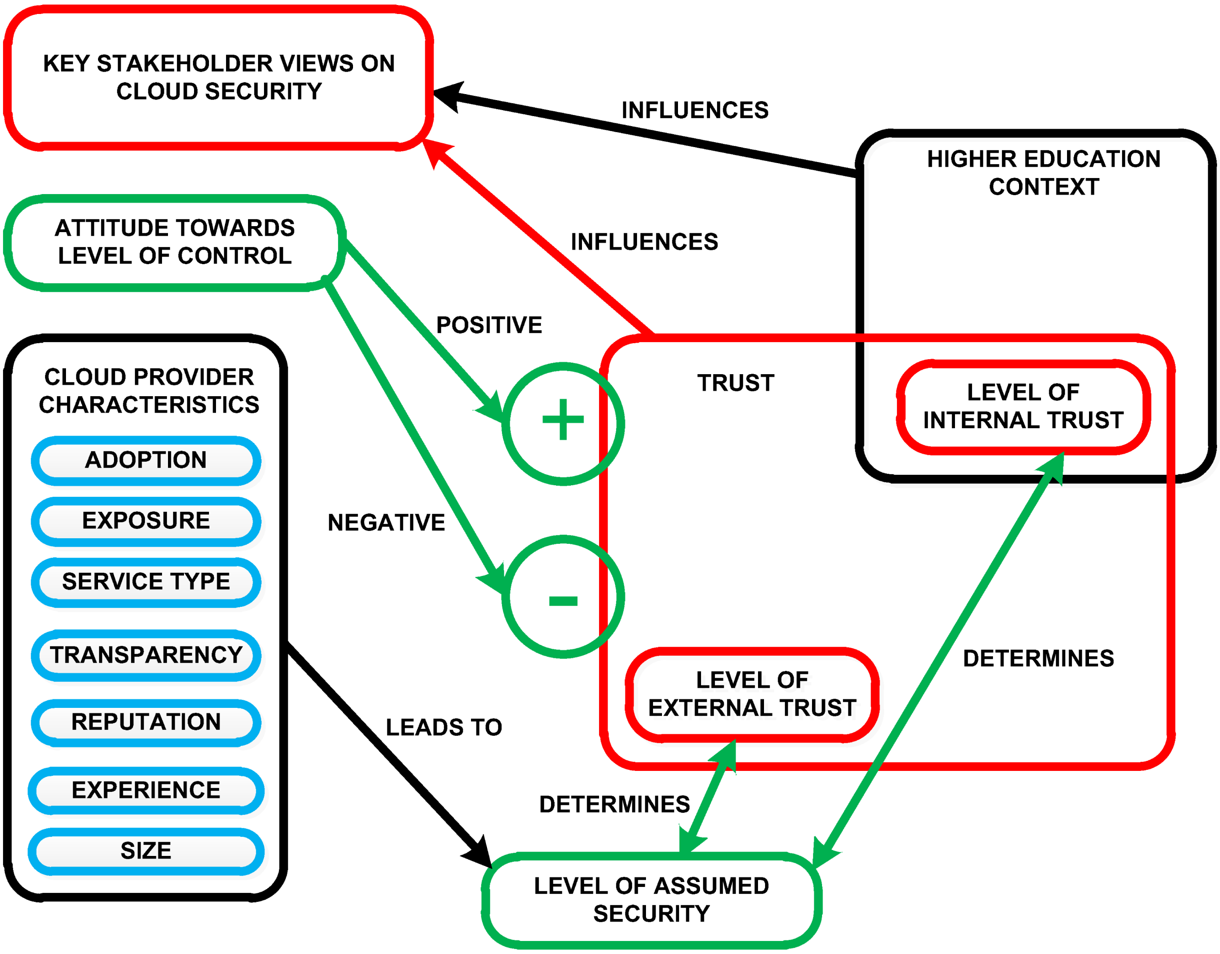


Figure 4.6: Conceptual framework of trust as a main theme

Security by Assumption

As one of the more prominent sub-themes, *"Security by Assumption"* is defined by the fact that many of the participants assumed that information security is a priority for cloud providers. Participants appeared to assume information security was considered during the evaluation of the cloud; a process internal to most organizations. The following statement by Participant L, from University C, demonstrates this:

> *"I wasn't part of that evaluation process; obviously security must have been."*

Assumptions such as those presented above would make sense in a scenario where the participants do not have any direct contact with an evaluating committee. There are three aspects to this which is noteworthy. First and foremost is the fact that a department who is considering migrating to the cloud should involve senior members of staff; especially key stakeholders with a technical background. Secondly, it would seem that these assumptions are also taking place on the level of the evaluating committee. Thirdly, with University C being classified as a research intensive university it also shed some light on the assumptions that are made about the knowledge post-graduates and academics have with regard to cloud security. Interpretation of these assumptions leads the researcher to infer that:

- Internal communication does not take place between the evaluators of the varying cloud solutions and the future users of the cloud solution,
- The participant implicitly trusts the evaluating committees' judgement in this regard and/or
- This university deems its post graduates and academics to be well aware of cloud security, so much so that the evaluation process does not cover cloud security in enough detail to be known to all key stakeholders.

To participants from University A, the concept of *"Security by Assumption"* took on a more pronounced form, with most of the participants discussing some aspect of this sub-theme. The researcher concludes that this could very well be because they have been successfully providing this service for such a long time, which has instilled confidence in most of the key stakeholders. This in turn affects their levels of trust as a cloud subscriber. In essence the confidence and experience gained from providing a cloud infrastructure has positively influenced their views on the subject of cloud security and trust. In *Figure 4.6* this sub-theme is illustrated by the concept *"Level of Assumed Security"* where the relationships between it and internal as well as external trust is depicted. The reader will note that these relationships are two-way in nature mainly because the interview data indicated that the levels of trust also had an effect on the assumptions participants made with regard to cloud security. Importantly, none of the participants made a clear connection between the concept of cloud architecture and cloud provider trust. As such, cloud architecture has been removed from the conceptual framework illustrated in *Figure 4.6*.

With University B having used their cloud solution for quite some time, their focus is understandably operational in nature. Their assumptions made about service providers reflect this. Although no real auditing is provided by their service provider, the assumption is still there that the said provider takes information security seriously. This is confirmed in the following statement by Participant G:

> *"I think fair use and abuse and those sort of things are highlighted or the understanding is that [Provider F] endeavours, because they [are] offering a service, they endeavour to do everything in their power you know to make sure that that's not being abused or open."*

The absence of issues directly related to cloud provider trust, together with the fact that they have not experienced any known cloud related incidents, makes it apparent that the use of their cloud solution has had a positive effect on their views on cloud security. Another factor which could explain the positive attitude could be the fact that they have a post dedicated to information security. The presence of this person could be interpreted as a form of internal trust. Even University A exhibits forms of internal trust. For University A this has been more pronounced. Their steering committee did not have any major information security concerns regarding cloud adoption. The following statement from Participant E captures the essence of this:

> *"... the only concern that has ever been raised is what happens when the Internet goes down, which astounds me."*

From this the researcher infers that there is not only a level of trust between the steering committee and the architects of the proposed cloud solution, but also a general lack of awareness regarding information security. This exhibits an even deeper level of trust on a wider scale. Not only are the subscribers or users of this system trusting the architects (key stakeholders), but in doing so there is an implicit trust relationship between the users and the cloud provider. From a user perspective Participant D had this to say:

> *"... there's elements of trust and the idea of a pre-packaged solution like [System A] sort of thing it's a sort of thing that out there it's working and basically when was the last time I worried whether my private personal [System G] stuff was backed up or not."*

As such the concepts *"Internal Trust"* and *"External Trust"* are depicted as components of the core concept, namely *"Trust"*. In the context of this study these components (*"Internal Trust"* and *"External Trust"*) encapsulate where the *"trusted"* party resides from the perspective of either the key stakeholders or the participating universities. As such the term *"Internal Trust"* refers to trusting parties within the university itself. On the other hand the term *"External Trust"* refers to trusted parties residing outside the participating university's operational context. The overlap between trust and the concept of *"Higher Education Context"* is indicative of the varying contextual factors upon which internal trust is based.

The concept of trust does not only apply to the general aspects of information security, but also to some very specific areas. Many of the participants were able to articulate exactly where trust factors into cloud information security.Bearing in mind participants in managerial positions mentioned aspects reflecting their operational context, which was not technology or vendor specific. Participants with a technical background made more references to the actual mechanics of information security, although not as in-depth as the researcher would have expected. Other than internal trust the specific areas addressed by the concept of trust more often than not involved factors external to the the participating universities. These areas of external trust include:

- **Trusting cloud providers in terms of the API's they provide to their subscribers:** This was one of the few instances where a participant made reference to an area of concern mentioned in the literature. The literature covered in *Section 2.5* specifically mentions that the existence of insecure API's should be seen as a threat. If on the one hand the subscribers trust providers to supply them with secure API's it becomes plausible that subscribers inadvertently use this form of external trust as a means of threat mitigation; possibly without even thinking of it as such.
- **Physical access to the cloud provider's infrastructure:** With regard to physical security Participant C (from University A) stated that it is fair to assume that the same rules and regulations are in place at the provider as is on their site. The existence of any additional threats is accepted at face value and only experience will be able to confirm whether or not these assumptions were indeed incorrect.
- **Trusting the cloud provider to back up subscriber data:** Participant A specifically mentions that there is no certainty as to whether the cloud-based data is backed up. This does not deter this participant from assuming that it is being done and relates directly to what is specified in the service level agreement between a university and their cloud provider/s.

So, over and above the external trust relationships between the cloud provider and subscriber there are other more intricate trust relationships internal to the some of these universities. Interpretation of the interview data has lead the researcher to infer that these trust relationships are based on assumptions when the following holds true of cloud providers:

1. The cloud provider has a good reputation;
2. The cloud provider is considered to be of substantial size;
3. Subscribers (key stakeholders) view them as experienced and mature;
4. They have acceptable levels of transparency;
5. Levels of exposure from the institutions' (as subscribers) perspective lends itself to such an assumption;
6. Their services are not free and/or
7. Their services have already officially been adopted

Some of these core criteria are depicted in *Figure 4.6* under the concept *"Cloud Provider Characteristics"* and from the interview data they seem to be the initial reasons why key stakeholders assume security, hence the relationship with *"Level of Assumed Security"*. The operational context of University B, as well as their choice in provider, corroborates the first five criteria on the aforementioned list. In their instance the fifth criteria does not apply, since their cloud provider offers them their service free of charge. As mentioned earlier University B also has a post dedicated to information security. This would allow them to make informed decisions about some of these criteria; especially those criteria which require specific industry exposure. It is more likely that the incumbent of such a post would have regular contact with other information security professionals, allowing him or her to base their decisions on an even larger knowledge base.

For a university such as University C the list of criteria is less operational and more preparatory in nature, since they are only evaluating the cloud. With some of the participants stating that they were supposed to have implemented their cloud solution already the researcher infers that this could very well be related to the cost of Internet access. From this perspective University C is unique in the sense that Internet access or data is not supplied to students free of charge. So, it is plausible that at this stage the above criteria do not play such large role as with the other two universities.

The operational context of University A is a mixture of both the other universities included in the study, in the sense that they are evaluating and using the cloud, albeit for different systems. Their experience as a cloud provider also adds credence to the views of the participants from University A, since these views are based on external trust, internal trust and most importantly being trusted by the other members of the community cloud. The participants from University A mentioned trust the most. The researcher believes this can be attributed to their mixed approach to cloud computing. This mixed approach is not only defined by their use of different clouds for different systems, or evaluating the cloud versus adopting the cloud, but also the use of free services as well as services which are not free. Another factor that distinguishes University A from the other universities is the sensitivity of the data that has been hosted by cloud providers. In this instance University A hosts most of their sensitive data with providers who charge for their services.

This leads the researcher to infer that participants make a lot more assumptions about the concept of trust and information security when they have to pay for a cloud service. This is depicted in *Figure 4.6* as the term *"Service Type"*, which forms part of the cloud provider characteristics leading participants to assume security. There is also an expectation that these cloud providers are more likely to be transparent; especially with regard to information security. In general it would seem that if a cloud provider satisfies a number of the aforementioned criteria (see page 78) participants assume their information is secure. Given enough time this develops into a sense of trust in the cloud provider. Another key criteria in the list above is whether or not a cloud service has officially been adopted or not. Its importance in this argument is illustrated by the fact that the universities who have been making use of cloud services are more positive about adoption and cloud security. This is especially true of University B who has officially adopted the cloud for some services. From the interview data of University B the researcher infers that, because their cloud solution and operational context satisfies many of the criteria above, their positive views on cloud adoption has enabled them to assume that their information is secure. This in turn leads to a sense of trust in their cloud provider.

All of the concepts that make up this sub-theme have been illustrated in *Figure 4.6* as well as their relationship to the concept of trust. Various cloud provider characteristics are depicted which is related to the list of criteria discussed earlier. The assumptions made from these characteristics leads to the assumption that the cloud provider is secure. Given enough time (post cloud adoption) university key stakeholders develop a sense of trust in the cloud provider, influencing their views on the security of cloud-based information. Context also influences key stakeholder views, hence the relationship between the concept *"Higher Education Context"* and *"Key Stakeholder Views on Cloud Security"*.

In the conceptual framework derived from the literature (see *Figure 2.3*) no explicit references are made to the concept of trust. Moreover, none of the survey or interview questions directly addressed the concept of trust. The issue of trust thus emerges as a significant contribution to understanding the cloud.

Loss of Control

During the phases of analysis it became evident that participants either viewed control over a cloud infrastructure (or lack thereof) negatively or positively. For this reason control, at least from the participant's perspective, has strong connotations to the concept of trust. This is illustrated in *Figure 4.6* where the level of trust, whether it be internal or external, is either increased or decreased. A negative attitude towards cloud control decreases the levels of trust whereas positive views increase levels of trust. Several data extracts confirmed this. Specific areas of control include:

Control over cloud-based data: The researcher interpreted Participant A's views on the loss of control over cloud-based data as positive in nature. According to this participant they never lose control over their data. This is attributed to the fact that they have backups; once again an issue relating to trust on the part of the participant:

> *"... between [System B] and [University A] is a stipulation that they do two backups, so yes those backups are run and they are then... I think one is on campus and I think the other one is off campus. I'm not sure, but I trust them."*

The literature reviewed in *Section 2.5* makes specific mention of backups as a means of protecting an organization from data loss or corruption and is thus seen as a form of mitigation. It is further suggested that backups be controlled contractually, which is true for the example above. This translates to trust on an external and internal level. It's external in the sense that as a subscriber, such as Participant A, there is an assumption that the provider makes backups. On the other hand it's also internal in the sense that the participant trusts the university's internal resources (possibly other key stakeholders) who entered into the agreement. This form of internal trust would encapsulate whether or not these internal resources performed with due diligence during the evaluation process. Assuming that there was an evaluation process. Thus, as long as there is an agreement in place through which this university can control its cloud-based data (via backups), the levels of internal and external trust increases. This in turn warrants certain assumptions to be made, which in this instance pertains specifically to the security of their cloud-based information.

Mechanisms of control: Participant M stated that control or the loss thereof is not a concern, since there are mechanisms to deal with such situations. These mechanisms include choosing a provider that matches your requirements, assurances from providers as to the levels of service and the security they offer. Choosing vendors who understand the industry is also mentioned. With University C only evaluating the cloud at this stage it is fair to say that the level of experience they would have with the aforementioned mechanisms would be limited. Especially within the cloud. Furthering this, although such mechanisms could result in adequate levels of control the latter two rely heavily on the amount of cloud provider transparency. This in turn equates to certain security assumptions being made in relation to the level of transparency.

The control over these mechanisms, based largely on assumptions (and levels of transparency), is interpreted as having a positive effect on the levels of trust. The concept of internal trust within the context of information security takes on a different meaning for some participants at University C. Research output is seen as the most valuable information asset and yet it is believed to be unprotected, as stated here:

> *"... that stuff [research] is the most unprotected of the lot."*

Here an assumption is made about the insecurity of the cloud-based data. With some of the institutional data already in the cloud these mechanisms become personalized, since the products mentioned in the following statement are consumer based:

> *"... you find that much of your research information is actually sitting out there synced to [System I] and [System K] and [System J]... "*

Choosing the correct cloud provider is done at the user level and not at an institutional level. This in turn requires internal trust not so much in the decision making abilities of internal resources, but rather in the way the cloud-based information is used.

Provider-based control: From an operational perspective participants from University B still view the loss of control over their cloud as an issue. So much so that the cloud is not being considered for staff members. The fact that they have yet to encounter any serious issues with their current implementation makes this an interesting point of view, since this in itself should bolster their levels of cloud provider trust. From several of the interviews conducted at University B it was clear that the physical location of data is also a concern. So in essence the provider has direct control over where the data is located and indirect control over bandwidth and legal matters. Of the three the amount of bandwidth dominated over legal concerns, especially from participants with a technical background. Those participants, operating within a managerial role, viewed the legal implications as an issue that needs to be addressed.

It is however important to note that both bandwidth and legal concerns are directly affected by the physical location of cloud-based data. Within the context of University B it is entirely possible that it does become a concern with time (i.e. with experience). Thus the fact that providers have control over specific aspects of a cloud infrastructure should make participants view the loss of control as a negative. However, Participant G had the following to say in this regard:

> *"It's not that they don't trust you. It's something they control across the whole platform of services. They don't want you to damage this or break this component of [System H]".*

This statement implies that Participant G views the loss of control as a means of protection, which cloud providers employ to protect themselves from cloud subscribers. Here the loss of control, as a function of trust, is seen as a positive. The fact that this specific participant does not view this as a form of mistrust from the provider's perspective could be explained by this participant's strong technical background. This interpretation implies that providers have varying levels of trust. In essence the assumption by Participant G that the loss of control results in a system he can't damage increases the levels of trust he places on the extent of his abilities not to damage the system. The same holds true for the provider with the only difference being that the provider does this by increasing his level of control.

The concept of control is depicted on the new conceptual framework as an attitude that a key stakeholder has towards the amount of control they have over their cloud infrastructure. If they have a positive attitude they trust the provider more, whereas a negative attitude detracts from the amount of trust key stakeholders place in cloud providers.

In most cases during this study participants viewed the loss of control in such a manner that it resulted in a decrease in the level of provider trust. Within the context of this example this is not the case. In fact the participant even confirms it in the aforementioned statement. Its just the level of trust which differs.

As a main theme *"Cloud Provider Trust"* is, as demonstrated, influenced by subscribers either assuming some level of security based on some presuppositions as well as the level of control key stakeholders view themselves to have over the cloud. This affects the views key stakeholders have on the subject of cloud security. With this theme being very provider focussed the following theme that emerged was more subscriber focussed and able to give a more complete picture of the views key stakeholders have with regard to cloud security.

4.4.2 Views as Subscribers

As opposed to the other main theme illustrated in *Figure 4.5*, the following main theme comprises more direct views on the core concepts of this study. Much of the data gathered during the interviews was limited to the views expressed by the various participants within the limitations on what these participants were able to comment. This in turn relied on the knowledge and experience each participant had with regard to cloud computing. The concepts that constitute this main theme is illustrated in *Figure 4.7* and together with the thematic map (previously shown in *Figure 4.5*) will form the basis of the discussion to follow.

Security of Cloud-based Information

During many of the interviews it became apparent that participants viewed only certain types of systems and data as suitable for cloud computing. More often than not data considered valuable (or critical) to the university were deemed unsuitable to the cloud. Although these motivations are affected by the security context within which these systems operate, they are fundamentally based on the level of understanding, knowledge and awareness participants and users (students and staff) have about cloud security. The following statement, by Participant E, captures this sentiment:

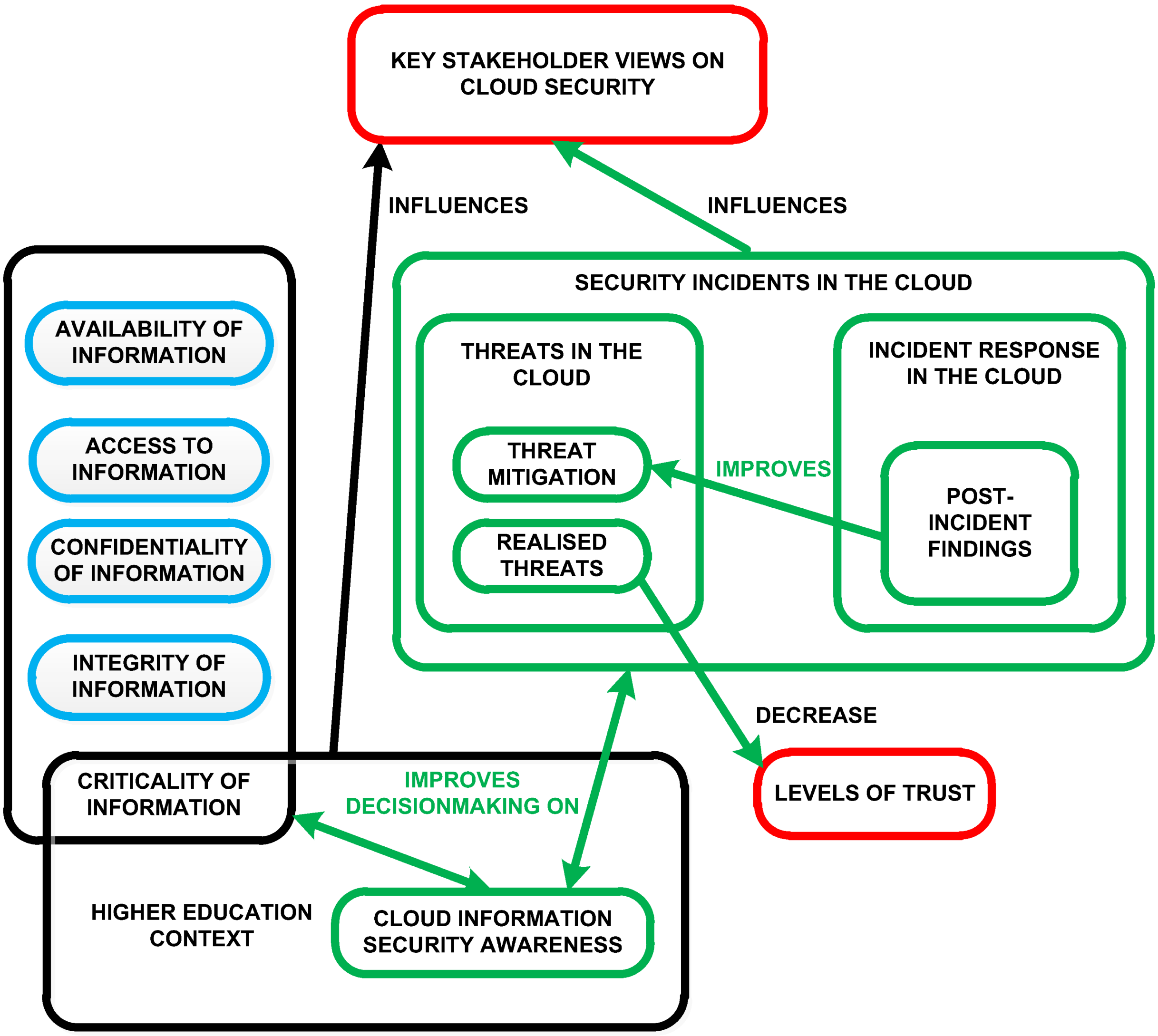

KEY STAKEHOLDER VIEWS ON CLOUD SECURITY
INFLUENCES
INFLUENCES
SECURITY INCIDENTS IN THE CLOUD
THREATS IN THE CLOUD
THREAT MITIGATION
REALISED THREATS
IMPROVES
INCIDENT RESPONSE IN THE CLOUD
POST-INCIDENT FINDINGS
AVAILABILITY OF INFORMATION
ACCESS TO INFORMATION
CONFIDENTIALITY OF INFORMATION
INTEGRITY OF INFORMATION
CRITICALITY OF INFORMATION
IMPROVES DECISIONMAKING ON
DECREASE
LEVELS OF TRUST
HIGHER EDUCATION CONTEXT
CLOUD INFORMATION SECURITY AWARENESS

Figure 4.7: Conceptual framework of key stakeholder views as a main theme

> *"I think most of them don't even know what you're talking about. I'll say the same for staff too. My experience is that South Africa in general is very naive about Internet security. That applies across the board."*

For a university such as University A, which is only starting to use some of the features of their cloud solution, it is understandable that information security awareness would be of concern. The following statement from Participant B also captures much of what has been said above:

> *"I want to think about that carefully simply because I'm not so much sure that it's a case of caring as opposed to understanding. So I think if they knew all the issues they would care, is kind of the point,*

> *but I'm not sure that they necessarily understand all the issues and therefore what might seem like them not caring is simply a case of them not understanding..."*

From this one can see that issues such as confidentiality, integrity and availability of cloud-based information are not a priority with most university students and staff alike. Participants from University B did not all view awareness as an overall good idea. Coming from a university which has already adopted and used the cloud this is a unique view; one that is not shared by the other participating universities. Although University B's participants did not mention any specific security incidents, the operational experience that some of the participants (e.g. Participant Z) have leads them to believe that a campaign of security awareness might be more risky than not doing it in the first place. Participant Z might also feel that the risk of someone becoming overly concerned about cloud security would be greater if they are actually using it in-depth.

With University A only partially using the cloud and University C evaluating it, the researcher infers that awareness is not too great a concern at the moment simply because cloud services have not been used extensively. However, the interview data led the researcher to conclude that most participants from University A and C viewed awareness as a vehicle towards adoption. For this reason the conceptual framework depicts awareness as a means to make informed decisions about security incidents as well as the criticality of information. Both components are deemed crucial to a successful cloud adoption campaign.

Concerns about the security of cloud-based information change, not only according to the type of information being stored or accessed, but also by whom this information is used and for which purpose. Participants from University A viewed postgraduates as having a much more concerned attitude towards the security of their research as a whole. With the majority of participants viewing research data as the most valuable information asset, most participants deemed such data as an unsuitable candidate for hosting in the cloud. The reasons for this are depicted in *Figure 4.7* under the heading *"Criticality of Information"*. The overlap between the latter concept and *"Higher Education Context"* is indicative of the underlying contextual factors that determine the criticality of information. For example, some of the participants job functions gave them a different outlook on availability. Another example would be University B not mentioning the use of a community cloud, hosted by University A. The importance of these two concepts warrants an in-depth discussion on each of the reasons depicted in *Figure 4.7*.

Retaining access to institutional information: Within the universities which have not fully adopted a cloud solution, this seemed to be a concern that at least a few participants shared. For University C these views stem from the experience other universities have had in this regard. In this particular instance the cloud subscription had lapsed and the university in question was not able to access their cloud-based research information. Examining this further reveals that it is not only a concern related to cloud security, but also to the fallibility of administrative processes and policies. This specific concern might be motivated by the lack of confidence in the administration of University C, since there is the fear of a similar situation arising (lapse in cloud subscription). This also affirms that participants make a clear distinction between cloud-based information which is almost dispensable and those which are not, such as research information. Another participant from University C refers to this as *"Alienation of Information"*, which infers that there is not only a concern related to accessing cloud-based information, but also the loss of ownership of such information. Within the context of University C this viewpoint might very well also be motivated by the possibility of a cloud subscription not being renewed. Only in such an instance would ownership of information come into play. In fact this then becomes an underlying legal concern, which is directly affected by the physical location of the information in question.

In line with this, Participant B raised the concern that there is a lack of clear policies which address emergency access to information within University A. As opposed to the latter concern this is largely outside the direct control of universities, because it addresses access to information where the owner of the information is no longer available to transfer ownership thereof. This is especially likely if participants make use of consumer cloud solutions which are not under direct control of the university. From this the underlying concern might very well be related to the fear that the cloud has already been adopted at an end user level. Making it difficult to change the way these end-users store and access cloud-based information. The following statement by Participant B, enforces this argument:

> *"You know if you say now we not gonna adopt the cloud, the users are gonna adopt it for you."*

These concerns are not shared by participants from University B. Then again, University B is not hosting core institutional information in the cloud, as stated by Participant Z:

> *"There was you know initially the hesitance in sort of where the data's stored, who's gonna have access to the data, but being with, it with [Provider B] we felt safer... and also the sort of data that's there is, it's basically emails. It's not the research..."*

Another important aspect of the previous comment is the fact that Participant Z views their particular cloud provider as a safe haven for the type of data that is hosted there. Indirectly this confirms what was previously said in that the cloud is viewed as only suitable to certain types of information. Clearly emails are either not that critical or Participant Z deems their particular provider as an expert in hosting such information. This in turn suggests that from experience University B's key stakeholders view certain cloud providers as experts in only certain areas of cloud computing security. This sentiment is echoed by Participant E (from University A) who, in addition to the latter, views the security of certain types of cloud-based information as a function of the amount of information that is based in the cloud, as well as its relative criticality.

Availability of cloud-based information: As a concept, availability seemed to be viewed differently depending on the context within which the participants operate. Technically minded participants placed much more emphasis on the availability and reliability of the connection to the Internet. In some instances those employed in a more managerial role viewed availability as another word for resiliency. This reflects a very business-like approach to the cloud. Availability ranked highest amongst the universities who are officially using the cloud. Only a handful of participants from University C and University A viewed availability as a concern, which is evident from this comment by Participant E:

> *"... availability is at the bottom I think. Availability is easier to mitigate."*

Of course these views are impacted by the amount of time that has passed since they have been connected to SANReN. This is a logical conclusion, since SANReN is seen as a key enabler (Participant B) to cloud adoption within higher education:

> *"Oh it, it's a huge enabler"*

With almost all of the threats listed under *Section 2.5* resulting in the loss of availability, either directly or indirectly, it becomes clear why some participants viewed it as a primary threat although it is probably more akin to a risk. Although the literature suggests that providers make the needed changes to their infrastructure, in an effort to ensure the availability of cloud services, participants viewed this as something that depends on provider transparency. The fact that auditing of cloud services is not taking place (in the case of University B) makes some mitigation techniques, such as those presented by Molnar and Schechter [59], of little use to University B.

The results from a survey, conducted by the Data Security Council of India [25], do not correlate with many of the participant's views regarding the effects availability has on the security of cloud-based information. In this survey only 24% of participating organizations rated the availability of cloud-based services and information as a critical area of concern. The researcher infers that although these results were obtained from another third world country, these different views might be attributed to any combination of the following:

- More bandwidth being available to these Indian participants;
- More cloud experience and knowledge on the part of these participants;
- Cultural differences resulting in a different outlook on the concept of availability;
- Differences in the amount of funding available to implement mitigating strategies and techniques;
- Organizational differences and/or
- Less critical applications and services being hosted in the cloud

Similar results were found by the Ponemon Institute [68]. The fact that these participants were based in first world countries lessens the applicability of some of the reasons listed above.

Confidentiality and Integrity of cloud-based information: The researcher has decided to group these two core information security concerns in an effort to reflect how little was said in this regard. Even from the small scale survey (see *Section 4.2* on page 62) it was evident that availability overshadows these two concerns. During the interviews it seemed that the confidentiality and integrity of cloud-based information was even less important than what the survey data suggested. However, the confidentiality and integrity of cloud-based data does become a concern when sensitive data is stored in the cloud. This is yet another indicator that the type of cloud-based information makes a difference when it comes to the concerns expressed by the participants. For University A confidentiality seemed to be a concern depending on the security context of the information. The sentiment here is that if cloud-based data's confidentiality is not compromised and its more available then that is acceptable, as stated by Participant F:

> *"I would say confidentiality first, probably integrity second. Availability. . . [there] is enough redundancy if you, if copies here and there; it's centrally stored on your laptops. Certainly I would rather protect confidentiality first and have a risk of an availability loss than making it too easily available."*

The relationship between the confidentiality and availability of cloud-based information becomes evident in this example. From this the researcher infers that University A's experience as a cloud provider has taught them that there is a fine line between the confidentiality of information and its availability. This is understandable, since when information is made available to a subset of users its no longer as confidential as it was before its availability was increased. Its almost possible to say that in some instances the availability and confidentiality of information is inversely proportional. In a cloud there are countless measures to control access to information, such as passwords and access control lists, but in principle participants viewed the confidentiality of cloud-based information in much the same way. With the research data being viewed as the most important information asset. Participant Z had the following to say in this regard:

> *"Well research is very sort of you just don't want people to have access that shouldn't have access to it. That has to be kept close under the arm."*

Participant M, who is employed by a research intensive university, had a completely different view in this regard:

> *"I would say availability. The reason I say that is because if I think about research information a large proportion of that information should be [seen] as being funded by public money and should be in the public domain."*

After all if the integrity of your research data is questionable it has a direct negative impact on any research outcomes. To a university, which is essentially an institution dedicated to research, this is of vital importance. This does not preclude some participants from having unique views on these concerns. Those participants involved in the dissemination of information viewed the security of information in a staged manner. To this participant the confidentiality of information is of vital importance during the initial stages of production. Once this is complete confidentiality becomes less of a concern, since the focus shifts from withholding the information to distributing the information to its intended audience.

Together with the concept *"Criticality of Information"* the concept *"Higher Education Context"* influences the views of key stakeholders on cloud security, as illustrated in *Figure 4.7.* From the perspective of the literature (see *Section 2.5*) subscribers may have some questions to ask their provider regarding the confidentiality of their information. Especially when they sever ties with the specific cloud provider. This was not mentioned by any of the participants with the most likely explanation being the fact that none of the universities have been using the cloud long enough. In addition to this none of the participants mentioned that they have ever severed ties with a particular cloud provider. Although Bradshaw *et al.* [9] specifically refers to certain contractual elements, which contain details of the above none of the participants stated that they have inspected their terms of service in any detail. Having articulated the reasons or factors that determine the criticality of information as well its interdependence on the context the researcher now needed to investigated how participants viewed security incidents within the cloud.

Information Security Incidents in the Cloud

Early on during the interview process it became apparent that cloud computing threats, threat mitigation as well as the incident response life cycle are entwined in such a way that it would make sense to discuss them as a cohesive theme. As such *Figure 4.7* depicts the concept *"Security Incidents in the Cloud"*, which contains components related to threats and as well as security incident response. The reader will notice that, with regard to threats and security incident response, not much has changed from what is illustrated in *Figure 2.3*. The interview data corroborated the literature in that most participants viewed the last phase of the security incident response life cycle (post-incident findings) as a means to improve threat mitigation. All of the aforementioned components contain elements which:

- Affect the level of cloud provider trust and
- Are controlled externally, internally or a combination of both

As such *Figure 4.7* indicates that realised threats decreases the levels of cloud provider trust. To expand upon these general concepts, as well as their relationships with each other, the researcher must discuss the participants' views on threats and security incident response within the a higher education cloud.

Threats in a Higher Education Cloud: For an overwhelming number of participants internal threats were viewed as the most critical area of concern. Some external threats were mentioned, such as a complete loss of cloud-based information, as stated by Participant G:

> *"... the biggest threat would be loss of data number one physically loss of data in other words your datacentre goes bang and everybody loses their stuff."*

Almost all the external threats mentioned came from participants in the employ of University B. From this it is possible to infer that as University B gained experience (as subscribers) with their cloud solution the initial tendency to be concerned about internal threats were replaced by those external to the university. In fact data loss within an external security context was the only external threat mentioned. For some participants vendor lock-in featured as a threat although the literature regards it as more of a risk. As far as data loss is concerned the literature states that the loss of data can have a number of negative side effects. Prominent amongst these is the loss of trust, as discussed earlier. From the above it follows that threats also have a role to play when it comes to the amount of cloud provider trust. With a realised threat resulting in some form of incident response one can see that even incident response is indirectly related to cloud provider trust. Most of the participants viewed their internal users as a threat. In some instances they specifically stated that it was their biggest threat. The internal threats mentioned included students as well as staff members and they were not always made out to be malicious as the literature suggests. Clearly behavioural factors also have a role to play:

> *"...but some of those threats originate internally because of the way users behave."*

Keeping the above in mind Participant E seemed to view the combination of user behaviour and availability as a catalyst for increasing one's exposure to cloud computing threats. This was the only participant who viewed the availability of the cloud as a threat:

> *"...because people do stupid things. The problem with this is that you increase your exposure. The inevitable thing about cloud services is that they work anywhere on the Internet"*

This viewpoint could be justified by two factors. Firstly, University A has been hosting a cloud and has as such taken much more time to evaluate all the possible avenues of attack. At the same time, they also considered the behaviour of their own users interacting with not only the public cloud, but also their own community cloud. It is plausible that this is the reason why none of the other universities' participants shared this point of view. As a provider University A's participants were also more aware of how cloud computing differs from other organizations. This stemmed from the fact that other organizations do not have students as users on their network. The fact that Participant E views the lack of control over students as a problem strengthens an earlier argument, which stated that in most cases the loss of control leads to a decrease in the levels of trust:

> *"...and so why are they my biggest threat? Because I've got no control over them. Not only do I have no control over them, [...] the difference is I don't have control over them and they're on my network."*

Though university A and C were evaluating the cloud they were able to anticipate that students may very well play a large role when it comes to actual threats to their cloud infrastructure. Participants from University B have a much more practical view on the threats posed by internal users. Their extensive use as only cloud subscribers has necessitated the need to monitor occurrences of authentication flooding for example. The differences in these points of view can be attributed to the fact that participants from University B made only a few references to the loss of control over their cloud infrastructure.

From the researchers previous arguments this is indicative of higher levels of cloud provider trust. This in turn negates the need to have a very threat-centric view of the cloud; as is the case with University A. With University C also lacking this threat-centric view of the cloud it becomes plausible that these key differences could be seen as turning points during the adoption process. Overall none of the other universities seemed to have thought through all of the threats in detail, since most of these detailed threat descriptions came from University A's participants. Being a cloud provider has obviously forced University A to evaluate these threats in greater detail than what a subscriber would do. From this the researcher infers that cloud subscribers:

- Expect their cloud provider to perform thorough analysis of any cloud computing threats, because they are the paid provider, and
- They assume their cloud provider is performing threat analysis and mitigation.

The above argument could be based on the fact that the subscriber does not have the relevant knowledge about the cloud and as such is not aware of the information security concerns. Remuneration also plays a role in these assumptions. After careful inspection of the threats listed in the literature, the researcher noted that some participants viewed these internal threats as a combination of malicious insiders, as well as the abuse of cloud computing. Participant F viewed students and their exploits as a means of gaining knowledge on how to improve mitigation. So, although some participants view students as a threat they are also viewed as a means to improve threat mitigation. This results in both the student and the university increasing their knowledge of the cloud. The only difference being the motivation behind these exploits. This point of view also originates from a participant employed by University A, whose prime directive as a cloud provider is to constantly learn how to better protect their cloud infrastructure.

None of the participants mentioned that they are particularly concerned about the amount of cloud provider transparency, especially not in terms of their employment practices. This opposes the views of Wrenn [94]. The Cloud Security Alliance [20] deems the abuse of a cloud infrastructure to only be applicable to infrastructure and platform as a service delivery models. This is contradicted by the fact that software as a service is by far the most popular cloud service model amongst the participating universities. Wrenn [94] does however make reference to the fact that malicious insiders could have a negative effect on the brand of an organization.

This is something that concerned Participant G (University B), stemming from the fact that their domain is embedded in all of the email addresses they host with their cloud provider. This, together with the fact that users are given the option of using these mailboxes for life, could lead to situations where the online conduct of certain individuals damages the universities' brand. The term *"Brand Association"*, as coined by Participant G, provides a unique perspective on the views certain participants have with regard to internal threats. The following statement captures this point of view:

> *"From a security perspective you always have the brand association which is number one so the [System H] service, although it is provided by [Provider F] in this particular case an external service provider. Which has its own policies and whatever, there is still the sense of brand association. In other words, the accounts are associated or the sub-domain would be..."*

This is not the case for University A and none of the participants made this connection. The early phases of adoption University C find themselves in also made it difficult for participants to make explicit reference to the above. Unlike the literature very few references were made to threats which are technical in nature. Instead participants viewed cloud computing threats in a user-centric manner with a focus on how threats could be managed or mitigated using contracts and agreements. This point of view was especially prevalent in the universities who have officially been using the cloud.

Mitigating Threats in a Higher Education Cloud: The views expressed regarding mitigation differed somewhat depending on the background of each participant. As a cloud provider University A's focus was based on safeguarding cloud-based information from inadvertent data loss. As such great emphasis was placed on the backup of cloud-based information. Participant E specifically mentioned this:

> *"It's all very well putting my data into your system and you guaranteeing me that you'll back it up, but how do I get backups out that I can keep?"*

The researcher noticed that the above statement not only addresses backups as a form of mitigation, but also has elements related to cloud provider trust. It is important to note that the above statement relates to how Participant E views backups as a cloud subscriber. Other participants from University A, in particular Participant A, also specifically mentioned backups, albeit in a different context. For Participant A backups of cloud-based information took the form of redundant clusters of information scattered around various data centres. Participant A further states that these data centres are in sync and thus provides some form of redundancy. For Participant A backups are thus entwined with redundancy, which offers the ability to seamlessly transition from a failed cluster to an active cluster. The fact that these clusters are hosted in different countries does raise questions relating to the legal ramifications of such a backup strategy. Although it is eloquent in nature this solution introduces more points of failure and relies on more external stakeholders than other methods of backup. These backup strategies do however address concerns around the availability of cloud-based information. The latter being a more effective way of ensuring this.

The above raises questions relating to how University B views mitigation, since they made no explicit reference of backups; especially not the data hosted by University A. Instead they made very general references to mitigation. This could be attributed to:

- Experience in so far that threat mitigation is seen as a responsibility of the cloud provider. Graphs such as those presented in *Section 4.2.3* provides some corroboration in this regard;
- The fact that they trust their cloud provider enough not to waste time on enumerating the various methods for mitigating cloud computing threats;
- The fact that the cloud-based information is not viewed to be sensitive enough to warrant an in-depth knowledge of the various mitigation techniques and technologies and/or
- Participants not realizing that they are in fact also making use of a community cloud and not just a public cloud.

The fact that none of the participants from University B explicitly mentioned System B strengthens the fourth argument, as stated above. The literature (see *Section 2.6*) makes specific reference to backups, but not in this context. Instead of directly addressing availability the literature references scenarios where backups are used to also mitigate against the loss of confidentiality. This is achieved by not only backing up the information (ensuring availability), but also encrypting (ensuring confidentiality) it. Participant F conveys exactly what the literature says in this regard:

> *"If you're using it for backup for example encrypt the files with your keys before you put them onto the backup, don't allow his encryption or his protection."*

Not allowing the cloud provider to encrypt the data on your behalf confirms that even this form of mitigation is only to be performed by a trusted cloud provider. In fact it is even possible to suggest that Participant F deems cloud provider encryption as ineffective and untrustworthy. As a participant employed by University A this statement is somewhat contradictory, since University A is itself a cloud provider. Of course from this participant's point of view this statement might only be valid when University A acts as a cloud subscriber. Other references to encryption are made, but these are used solely to ensure that the communication between two systems is secure. The latter is also referenced in the literature with the only difference that cloud providers should adhere to mechanisms driven by best practise.

As the literature suggests Participant G states that agreements should be used to provide some form of mitigation. What does differ is what it will be mitigating. For Participant G ensuring that regular audits be performed is of great importance. No mention is made of whether or not these audits would include evidence that backups and encryption are indeed being done. The emphasis placed on an operational facet of the cloud, such as auditing, is also indicative that participants view threat mitigation differently during the advanced stages of cloud adoption, as is the case with participants from University B. Only participants from University A explicitly mentioned the use of encryption as a form of protecting cloud-based information. Participant A made specific mention of the fact that encryption should also be used to secure data in transit (as suggested in literature), hence the use of Shibboleth as a form of securing communications. University A made no reference to encryption at all, since it is in a very early phase of adoption.

Most participants viewed these traditional threat mitigation techniques as valid in a cloud scenario. Having said this, with University B having extensively used their cloud solution; some of the participants made the connection between the physical location of the data and the procedures that would be required to mitigate in such situations. According to Participant G mitigation in the traditional sense of the word would have to be adapted because of this:

> *"We might have to especially seeing that the actual data is not sitting in South Africa as well. It does span borders. . . "*

Participant Z (also from University B) agrees with the above statement. For this reason it seems that experiential factors, such as the level of usage as well as the length of use, changes how participants view mitigation in the cloud. For University A the design of their cloud infrastructure is of vital importance when considering threat mitigation. In fact mitigation by design features strongest with University A, which is understandable with it providing a community cloud. Servers hosting the data and applications are secured and the system is designed with a strong focus on the concept of minimal trust. This mitigates the extent of any damage if a breach does occur. For the other universities design did not play such a big role, since they do not control their cloud infrastructure in such a way which would enable them to readily apply similar concepts as University A.

From the interview data it appeared mitigation by design did not feature strongly with universities who are cloud subscribers, but rather with universities acting as cloud providers. Once again the concept of trust (internal and external) comes into play. The design of the community cloud provided by University A was never questioned by University B and the literature does not mention design as a means of mitigation either. The lack of concern from participants of University B can be attributed to their reliance on another form of mitigation, which is mitigation by contractual agreement; a sentiment echoed in the literature where it is stated that cloud subscribers and providers should clearly communicate the terms and conditions of their service agreements. This also emphasizes the amount of trust they place on the agreements they have with their cloud provider. The following statement from Participant J adequately captures this:

> *"I suppose the guys you [are] getting the service from... there's a binding contract between you and that person, that service provider. So if there is something you know not above board then you've got the law on your side."*

The above statement also illustrates the fact that it is assumed that an agreement or contract will provide the necessary means of reducing any threats that may arise. This once again indicates that the concept of Security by Assumption plays a role even in the way key stakeholders view threat mitigation. In fact not only do participants assume security, but some also assume insecurity. Indicating that these assumptions are affected by whether or not a particular university acts as a cloud provider or subscriber. Together with the assumption of insecurity the concept of mitigation by design also indicates (at a deeper level) that as a cloud provider there is an understanding that even the best designs are fallible. It is quite profound that in this instance a reduction in the amount of internal trust would actually be desirable and also part of the design itself.

Another form of mitigation mentioned specifically by Participant G is carefully choosing the most suitable cloud deployment model; motivated primarily by the type of data to be hosted in the cloud. For University B any data related to or accessed by staff members should be hosted in a private cloud as opposed to a public or community cloud. This contradicts the fact that there is already a lot staff and research related information hosted by University A. Interestingly this is specifically what Participant M pointed out by stating that a large proportion of research output is already in the cloud. Such insight into the current state of the cloud within University C is indicative of a thorough evaluation on the side of University C's key stakeholders. Interview data also indicated that not only should the deployment model be carefully selected, but also the actual cloud provider. In line with this participants from both University B and University A stated that choosing a provider with a good reputation assists in providing an acceptable level of security.

From the above discussion it becomes apparent that university key stakeholders do indeed view some traditional threat mitigation techniques and technologies as useful, but that there are other more subtle ways of threat mitigation. It is exactly these subtle means of mitigation which indicates the difference in how higher education views the cloud as opposed to the business sector. These subtle means of mitigation stands in direct contrast with the very technology centric methods encountered in studies like those conducted by the Ponemon Institute [68]. Views such as those expressed by key stakeholders from University A originate from a deeper understanding of the cloud as a concept. A concept formed more from being a cloud provider than a subscriber. This is reflected in the technological nature of their views on threat mitigation.

For universities with experience in the cloud, mitigation becomes are more abstract design element; one which is relies more heavily on the amount of trust they place in the cloud provider. It is almost possible to say that the more experience is gained with cloud computing the more trust is earned by a cloud provider; essentially turning threat mitigation into a non technical concept.

Cloud Security Incident Response: As stated before in this study and especially the responses from participants who gave an indication that the concept of incident response, as well as, threat management is closely related. Not just in theory, but also in the way the participants viewed the relationships between these concepts. Of all the phases in the security incident response life cycle (see *Figure 2.2*) it was the last phase (post incident activity) that made this connection most apparent. For most of the participants this phase provided them with an opportunity to learn more about a specific incident as well as how to either introduce a new form of threat mitigation or modify and existing one. This relates to an increased level of understanding:

> *"I think that the critical part is the feedback loop into how you mitigate for the future, but there is also [a] very strong part of trying to say right what changed, what went wrong, how do we recover what's happened since this incident occurred? You know how do we understand what was done."*

Although many of the participants shared this viewpoint Participant M also specifically stated that it should not only assist threat mitigation, but that the learning experience it offers universities should also be used to become more proactive. This is yet another indicator that University C has performed a very thorough analysis of the cloud. It does also raise questions as to what type of cloud they intend adopting, since there is a limit as to how proactive one can be within specific deployment and service models; especially from a technical perspective.

The literature reflects this aversion from a purely technical view of cloud incident response. Rather than looking at specific technologies and techniques used during incident response it implores subscribers to do proper planning. Essentially, planning entails making sure both the cloud subscriber and provider understand what they expect from each other in terms of incident response.

For most of the participants the planning phase was not considered the most important phase. In fact for the majority of participants it was indeed the ability to effectively detect and analyse security incidents that were considered the most important. When asked to motivate their answer they all indicated that if you can't detect an incident there is no incident, which in their opinion circumvents having an incident response life cycle. As a view shared by participants from all the universities the researcher is unable to infer that some of these views are influenced by contextual elements within each university. What is apparent is that because none of the universities, who are officially using the cloud (University A and B), has experienced a known cloud related security incident, it has not prompted key stakeholders to assess the processes in more detail. So in essence the only explanation the researcher has for this disparity with the literature is simply their lack of experience in terms of dealing with security incidents.

To a large extent this has to do with how participants view the responsibilities of both the cloud subscriber and provider in terms of security incident response. For participants from University B detection and analysis fell into the jurisdiction of the cloud provider, since they do not have the required levels of access to effectively perform this function themselves. These comments together with the fact that they view this very same phase as the most important makes for an interesting combination.

From this it is possible to infer that they are not only trusting the cloud provider with their data, but they are also trusting the cloud provider with a critical phase in the security incident response life cycle. With University B never having experienced a security incident in their cloud (known to them), it is entirely possible that this point of view will change with time. For Participant E (from University A) the responsibilities, as far as detection and analysis is concerned, is dual. It is dual in the sense that the cloud provider should detect and analyse incidents on their infrastructure with the cloud subscriber detecting incidents on the data hosted with the provider. This clear separation could be attributed to their role as both a provider and a subscriber making it difficult to separate the two roles from the combined operational context. Participant E further states that cooperation is key for these processes to be effective:

> *"Cloud providers and their customers must co-operate about issues... in issues about security, because otherwise this whole model falls apart."*

Once again the maturity of the evaluation process within University C is illustrated with Participant M clearly stating that the preparation and post-incident activities should be done in conjunction with the provider. This is echoed in the literature (see *Section 2.7*), which states that preparation is key amongst all other phases. For some participants detection and analysis is nothing more than yet another reporting phase where the cloud provider issues a report upon the detection and analysis of an incident. Participant G furthers this argument by also stating that it would be counter productive to receive all breaches to security and associated incidents in real-time and that it should be done on an annual basis. This might stem from the fact that their cloud provider sends out regular communication in this regard, so much so that it provides too much information to process effectively. Participant Z shared these points of view. Therefore as stated earlier, if realised threats result in security incidents and University B identified agreements as a primary means of mitigating these, then for University B it becomes a question of how effective this agreement is. It also depends on who drafted the agreement and how transparent the cloud provider operations are when it comes to dealing with security incidents.

Some mixed views were encountered regarding containment, eradication and recovery. Participant G felt the processes involved in this phase should be applied internally as well as externally (at the cloud provider). This view could be explained by taking into consideration the context within which University B uses the cloud (email). Participant G specifically mentions abuse (spam) as a threat. This point of view makes sense, since there is a possibility that they would be able to solve this problem internally. Participant F (also from University B) echoed these views.

Participants who are charged with operationally managing University B's public cloud have a slightly different view whereby they state that containment, eradication and recovery falls within the cloud provider's jurisdiction. The literature elaborates by stating that containment, eradication and recovery differs depending on the chosen cloud deployment and service model. It is surprising that participants from University A did not have different views on this phase, which contradicts the literature in some sense. The fact that University A hosts a community cloud did not change the views of its participants, which indicates that participants either lacked knowledge of their participation in a community cloud or that they viewed it in a similar fashion as a public or private cloud.

University C's perspective about cloud security incident response is something that they have not dealt with enough to be able to have a solid viewpoint on. In fact some of the participants clearly stated this during the interviews. A clear case of any organization that has not officially used a public cloud. The cloud provider would be responsible for the detection and containment of any security incidents with the first and last phases falling within both the cloud subscriber and provider's jurisdiction, was stated by Participant M.

When dealing with actual incidents all of the participants stated that they would like to be informed of any breaches in security. Even if it was not directly affecting their data. For most participants the occurrence of such incidents does not constitute the need to jump from one cloud provider to the next. In fact Participant E felt disclosure of this nature would be an indication of a desirable maturity level on the part of the cloud provider. Such forms of disclosure, for Participant A, aids understanding in terms of how incidents are dealt with. The fact that both of these participants are in the employ of University A attests to the level of understanding required by key stakeholders from a university acting as a cloud provider.

The researcher would like to note that even here there exists a correlation between the level of experience with cloud-based systems and how detailed the views are with regard to cloud security incident response. Participants were able to logically evaluate the phases, but were not able to formally align them with what they are currently doing to combat such incidents. Of all the universities, University B had the most detailed procedures to follow in the event of an incident. University B is also the most experienced cloud subscriber of all three participating universities. Although the participants had little to say about the various phases of the security incident response life cycle, it is this very fact that indicates just how much they expect from their cloud provider. This in turn explains the low level of knowledge with regard to cloud security incident response. Within the context of threat mitigation and security incident response the following seem to be the norm:

- Agreements are seen as a form of threat mitigation;
- Post incident activity feeds into threat mitigation;
- The existence of low levels of knowledge on the security incident life cycle and/or
- A general lack of any formalized procedures for reacting to security incidents

The above findings shed light on just how well the various key stakeholders are familiar with their service level agreements. It seems to be assumed that these are drafted in a satisfactory manner; one that benefits them in their role as the cloud subscriber. From the discussions above it follows that *Figure 4.7* depicts the whole concept of *"Security Incidents in the Cloud"* influencing the views of key stakeholders with regard to cloud security.

So, not only has the reader been presented with a thematic map and a conceptual framework (see *Figure 4.7*), but also the interpretation of these themes within the operational context of each participating university. It is from these interpretations that the researcher will construct the findings of this study.

4.5 Summary

In this chapter the researcher presented the reader with the results of the online survey and a narrative comprised of the interpretations that were made during the analysis of the interview data. The reader has not only been presented with this narrative, but also the processes used to create the thematic map and conceptual frameworks upon which this narrative is based.

In the following chapter the researcher will summarize the findings of this dissertation with particular focus on how the research questions of this study has been answered as well as the contribution it has made to the field of cloud computing.

Chapter 5

Findings

5.1 Introduction

Using the interpretations provided by the previous chapter, it is the aim of this chapter to revisit the operational context of each participating university (*Section 5.2*) as well as to illustrate how the research questions of this study have been addressed (*Section 5.3*). A detailed discussion on the contributions of this study will follow in *Section 5.4*, with the researcher presenting a set of recommendations to South African universities in *Section 5.5*. Areas of future research are highlighted in *Section 5.6*, followed by a summary of the dissertation in *Section 5.7*.

5.2 Context Revisited

In *Section 5.3* the researcher provides explanations as to how each research question has been addressed. Although these explanations provide the reader with some background it does not contextualize the findings of this study for each participating university. This discussion aims to put these findings into perspective by highlighting how the researcher interpreted this study's central themes within the operational context of each university.

5.2.1 University A

As a research intensive university, University A is currently only using one component of their cloud solution. This places them between University B and University C in terms of the actual process of adoption. Most of the key stakeholders had a positive attitude towards using the cloud with some participants viewing it as a complete solution. Analysis of interview data which indicates participants' reluctance to adopt the cloud outright stems from the following:

1. Lack of clear guidelines with regard to information policy and
2. Difficulty to migrate both the students and staff onto the same cloud infrastructure. In essence getting everyone to use the same system.

Although participants stated that the policy issues is something that would have to be addressed it is unlikely that a quick solution will be found for the second point raised above. This stems from the fact that (mentioned by Participant E) the university consists of such a large number of departments with unique requirements. This makes it difficult to force one system upon the masses. Another component to this is the fact that university departments are given a choice as to whether or not they want to make use of a cloud service. Thus making it even more difficult to implement a single solution (staff and students alike). It is this contextual factor which sets University A apart from University B, who use the cloud only for some student information.

The progressive attitude these participants have towards the cloud leads the researcher to believe that cloud provider trust (a form of external trust) is not a primary concern for University A. Internal trust however, is a concern in so far that senior key stakeholders view internal users as a major threat. Some participants assumed their cloud-based information is secure, because providers are being paid for their services. These participants thus indirectly trust these providers. In many cases no distinction was made between critical and non-critical information, which might explain why the university participants did not go to the extra effort of trying to adopt different cloud solutions for staff and for students. From the researcher's perspective key stakeholders viewed both as equally important. It is plausible that this attitude towards the security of cloud-based information could be explained by their role as a cloud provider, which requires them to offer the same basic levels of service to all their subscribers.

As far as participant's views on threats, threat mitigation and security incident response is concerned the researcher could not find many resemblances in the literature. However, the ability to backup and retrieve cloud-based information did feature, which the researcher attributes to University A's role as a cloud provider. Participant views on internal threats mirrored those given by University B, with the exception that some senior key stakeholders at University A also considered the behaviour of their users. The researcher infers that this could be some form of trend analysis. Participant views on security incident response was limited and no formal procedures seem to be in place. From the perspective of a cloud subscriber this is expected, since only recently have they started using the cloud as a subscriber. From the perspective of a cloud provider it is indicative of their cloud subscribers,

- Not formally specifiying incident response procedures and expectations in a service level agreement,
- Their cloud subscribers simply trusting them as a cloud provider and/or
- A complete lack of awareness in terms of security incident response in a higher education cloud.

As they gain experience using the cloud as a subscriber this might very well change, since their perspective of the cloud now includes that of a cloud subscriber.

It is the researcher's belief that this is caused by a general lack of awareness with regard to the security of cloud-based information. During the interviews the researcher was not made aware of any campaigns to educate users on the security of their cloud-based information. This stands in contrast with University B which actively ran information security awareness campaigns. However, it is possible that University A's key stakeholders are waiting for the adoption of more cloud components before actively educating their cloud subscribers on the security of their cloud-based information.

5.2.2 University B

Almost all of the participants from this comprehensive university believed that their sensitive information (enterprise resource planning (ERP) system) is not suitable for the cloud. The researcher did not interpret this to be due to a lack of control, but rather availability as well as the fear of data loss within a remote cloud infrastructure. In fact, some participants from University B specifically stated that they would not even consider moving additional systems (more critical systems) to the cloud until Provider F starts physically hosting cloud-based information on the African continent. This was not interpreted to be the result of mistrust on the part of University B and as such trust seemed to factor less in the decisions of University B's key stakeholders. For the most part this seemed to be the result of evaluating their cloud solution using most, if not all, of the criteria presented in *Section 4.4.1* (see section titled *"Security by Assumption"*). From the researcher's perspective this is evident in the decision to only host a certain type of information (email) in the cloud for a subset of their users (students). This leads the researcher to believe that during the evaluation of possible cloud solutions, key stakeholders classified this type of information as something not critical enough to host on-site. Moreover, participants stated that students do not receive or submit critical information (such as assignments) via this channel (email).

Their views as subscribers, in terms of cloud computing threats, did not reflect the literature, other than reiterating the threat internal users pose as well as the potential for data loss. As for security incidents the interview data indicated that all security incidents follow the same channel, irrespective of whether or not it is cloud specific or not. When asked about the specific phases of the incident response life cycle the majority of participants viewed the detection and analysis of incidents as the most critical phase, with all the participants admitting that the last phase (post-incident activity) could be used to enhance threat mitigation. It is plausible that there has never been a need to evaluate cloud computing threats, threat mitigation and security incident response, since none of the participants indicated ever experiencing a cloud-based security incident.

For the most part University B's participants displayed a practical approach to the cloud. This resulted in some unique views on the cloud, which assisted the researcher in identifying several contributions to the field of cloud computing (see *Section 5.4*).

5.2.3 University C

As a research intensive university some participants had conflicting views on the security of cloud-based information, especially when compared with University A and B. For Participant M research material, although seen as one of the most important information assets, is unsecured. This stemmed from researchers making use of various consumer cloud services. Evaluating the concept of trust in the context of University C takes on two forms. On the one hand key stakeholders have to trust their users own good judgement in this regard and on the other hand they need to trust the providers of these cloud services. At this stage it is too early to evaluate this in context, since University C has not officially adopted any cloud services. However, from the earlier statement by Participant M it would seem that some of their users have already done this, albeit *"un-officially"*.

This could explain their reluctance to adopt the cloud. It seems key stakeholders first want to understand how the use of consumer cloud services will affect their adoption process going forward. Not only does the latter affect their adoption process, but also their approach to the allocation of Internet data. Unlike University A, for example, students are given a certain amount of Internet data which, when depleted, are charged to their student accounts. This differs from the approach taken by University A who essentially employ a rolling quota system, which allocates a certain amount of Internet data to each device a user registers on the network. All that is required when this quota is exhausted is to wait for the next quota window. With broadband Internet access seen as a cloud enabler University C is indirectly hampering the adoption of cloud services. Some participants did, however, state that this is something under review at the moment.

From the researcher's perspective University C is in a good position to successfully implement whatever cloud solution they choose. This stems not from their own evaluation process or any other contextual factors, but simply because they are able to learn from other universities in the South African context. In essence *Section 5.5* consists of quite a few recommendations on what South African universities should consider when looking towards adopting the cloud.

5.3 Research Questions Revisited

For the purpose of this discussion the researcher will be listing each of the research questions presented in *Chapter One* followed by the answers this study has uncovered to address these questions. First and foremost this study set out to address the following main research question:

> ***What are the views of key stakeholders within South African universities with regard to the security of cloud-based information?***

In this regard the researcher found that university key stakeholders had some diverse views on the security of cloud-based information. The interview data indicated that these views are, for the most part, defined by what this study refers to as their most important information asset. In fact, it is exactly this topic that is addressed by one of the sub-themes of this study, namely *"Security of Cloud-Based Information"* (see *Figure 4.5* and *Section 4.4.2*). For most key stakeholders the security of their most valuable information asset is of such importance that they do not deem the cloud to be a suitable option at this stage. Reasons for this include:

- Levels of acceptable exposure in terms of their most valuable information asset. According to most key stakeholders sensitive information (most valuable information asset) should be kept on-site,
- The levels of control they have over their cloud-based information, since for most key stakeholders these levels of acceptable exposure is directly influenced by the concept of *"Control"*. In *Section 4.4.1* the researcher demonstrated that most participants view the loss of control over their cloud-based information as a negative. The researcher also identified those key stakeholders who viewed the loss of control in a positive light and within which context these views were expressed.
- The concept of *"Trust"*, which is indirectly influenced by the concept of *"Control"*, as illustrated in *Figure 4.6.*

As indicated in *Chapter One* the process of addressing the main research question required investigating two sub-questions. The first of these sub-questions investigated the role cloud computing threats play with regard to the security of cloud-based information and was stated as follows:

> ***What are the views of key stakeholders within South African universities on how cloud computing threats affect the security of cloud-based information?***

For the majority of key stakeholders specific cloud computing threats did not affect their levels of trust and no direct relationship between threats and control could be made. In fact, very few references were made to threats the listed in *Section 2.5*, which is indicative of low levels of awareness and knowledge when it comes to the threats in a higher education cloud. Some corroboration of this can be found by inspecting *Figure 4.3*.

However, some correlation between the literature and the interview data was found in that almost all of the key stakeholders viewed their biggest threat to be internal to their university (see *Section 4.4.2*). Participant E equated the term internal threat to specifically denote students. From this it is inferred that Participant E assumes students to have a lot of time in which to probe the university network. In the case of University B students who specialize in information security were warned not to abuse the university network. The fact that key stakeholders felt the need to do this is indicative that students are viewed as a threat.

University B's key stakeholders viewed external threats in a more serious light than the other universities. From this the researcher inferred that experience using the cloud within their operational context changed their views on threats to be more outward focussed. From this the researcher inferred that given enough time universities seem to build up the necessary experience to focus on the bigger picture and to look at threats and threat mitigation from an internal and external perspective. For this reason some key stakeholders in University A and most key stakeholders in University B viewed threat mitigation as something more than just technological. Mitigating threats via contractual agreements is one such non-technical means of mitigation often mentioned during the interviews at University B.

University A also had some unique views on threat mitigation where, as a cloud provider, they deemed the design of a cloud infrastructure as a form of mitigation. The views of key stakeholders within University C were not as detailed due to the fact that they are still evaluating the cloud. So, in essence the views key stakeholders have as to how cloud computing threats affect the security of cloud-based information depends on their level of awareness, knowledge and experience as cloud subscribers as well as that of cloud providers.

With realised threats resulting in the need to deal with the resultant security incidents it made logical sense to also investigate the security of cloud-based information using the following sub-question:

What are the views of key stakeholders within South African universities with regard to the security incident response life cycle in a higher education cloud?

As for security incident response, few participants had any concrete views. Not to mention the actual security incident response life cycle. This is reflected by the low levels of experience with regard to security incident response in the cloud, as illustrated in *Figure 4.4*. The researcher inferred (from *Figure 4.4*) that most key stakeholders seem to expect their cloud provider to be responsible for incident response; hence the low levels of knowledge and experience. This was confirmed during the interviews. The researcher found that the universities who are still in the pre-adoption phase (such as University C) had limited views on security incident response in the cloud. The fact that University A acts as a cloud provider made the views of its key stakeholders in this regard more detailed (see section titled *"Cloud Security Incident Response"*).

The detection and analysis phase for key stakeholders within University B was most important and this sentiment was echoed by University A. For most key stakeholders the phases of the security incident response lifecyle requires the input from both the cloud provider and the subscriber. One aspect of security incident response that did stand out was the fact that all of the key stakeholders viewed the post-incident findings as a means to improve threat mitigation. For this reason it features on both conceptual models (see *Figure 2.3* and *Figure 4.6*) as a means of improving threat mitigation.

5.4 Contribution

Many of the contributions made by this study stem from the method that was used to acquire, analyse and interpret the primary data in the pursuit of addressing the research questions. Using the principles of interpretive field research the researcher was able to uncover unique aspects of this topic. Many of the aspects were directly related to the context of the participating universities. The terms *"Alienation of Information"* (University C), *"Brand Association"* (University B) and *"Emergency Access to Information"* (University A) are examples of the unique perspectives that emerged, lending credence to the in-depth and context-sensitive approach used in this study. This combined with the fact that the researcher focussed on institutions of higher education, has given this study a unique perspective on concepts which have previously only been explored with studies based on positivist paradigms. Methodologically the researcher contributed by slightly altering the methods used by Braun and Clarke [10]. These alterations included using the participant pseudonyms during data organisation, which aided the analysis and interpretation process. Instead of explicitly choosing to either analyse the data inductively or deductively the researcher clearly stated that they will be used in a combined manner, leading to a more comprehensive coding framework.

The aforementioned terms, and their context can be used by third party cloud providers to better understand the unique needs of South African universities. From this a range of services could be designed to address these needs and enhance cloud adoption within South African universities. This does not only apply to third party cloud providers, but also universities who are part of community clouds. Results of this study would be useful in the construction of a security driven cloud adoption framework. Such an artefact could be used by both cloud providers and subscribers.

This study also confirmed some aspects relating to cloud computing; especially the adoption thereof. It was found that university key stakeholders, in general, do not have a clear definition of what a cloud is; although most participants could articulate for what they are currently using the cloud. Most of them did not give the researcher an indication that they fully understand the potential it has for South African universities. Those participants that understood its intrinsic benefit did so by specifically stating that South African universities are too competitive and that it is this competitiveness which is withholding them from experiencing the collaborative power of the cloud. This study also uncovered the need for clear policies on how cloud-based information should managed and provided the reader with a set of criteria which, when fulfilled, instils trust in a cloud provider.

Quite a number of participants made calls for a larger community cloud to facilitate research and collaboration. They further felt that it was the duty of institutions, like TENET to facilitate this. The researcher interpreted these calls for a community cloud to be akin to the construction of a cloud similar in stature to that of SANReN itself. Also, having interpreted data from research intensive, as well as comprehensive universities, has led the researcher to conclude that there are only slight differences between the views of key stakeholders from universities with different purposes. The differences that were encountered was interpreted to be the result of the unique operational contexts of the participating key stakeholders. In fact, these differences are so minor that it leads the researcher to believe that the purpose of a specific university has little effect on the views expressed by the key stakeholders of this study.

Probably one of the biggest contributions of this study was discovering the emphasis key stakeholders placed on the concept of trust. This was not only exhibited by some universities or a select group of key stakeholders, making it an important contribution especially since none of the research instruments made any specific reference to the concept of trust. To explain how key stakeholders view these key concepts and their relationships with other concepts the reader was presented with several conceptual frameworks.

The researcher would like to point out that these contributions are not only theoretical in nature, but rather quite practical. These findings can be used as direct inputs to projects designed to address some of the findings highlighted above. In *Section 5.6* some of the projects which could make use of such inputs will be highlighted.

5.5 Recommendations

Before discussing areas of future research the researcher would like to highlight several recommendations for South African universities who have either started or are considering a move towards the cloud. As with most projects a successful cloud adoption process should be founded on frequent communication. This should not only be done internally amongst key stakeholders, but most definitely also the users of the intended cloud solution. With regard to communication the researcher would like to highlight the following recommendations:

- **Engage with users:** Key stakeholders should do this as early as possible. After all, these are the people who will be making use of the system and in turn either deem it a useful service or not. Such engagements should include awareness campaigns with a specific focus on the security of cloud-based information (University B did this). Surveys of what is currently being used, such as consumer cloud services, should also form part of this.
- **Engage with other key stakeholders:** This can take form of regular meetings or the establishment of a forum where matters of urgency can be discussed. It is important to note that these discussions should be widely attended. If a university is in a pre-adoption phase these type of discussions are vital, since they allow for the formation of information policies, guidelines, requirements (academic and students alike) and any further strategic decision making. Once adopted such meetings may not be needed as frequently and should exist to monitor what has been implemented and make changes as required.
- **Engage with cloud providers:** With unique needs and operational contexts it is important for South African universities to effectively communicate with cloud providers. The establishment of a country wide cloud consortium focussed on higher education could go along way towards fostering such forms of communication.
- **Employ specialised staff:** As seen in the case of University B, the presence of an information security officer enhances the adoption and operation of a cloud infrastructure. In fact, from the information gathered during this study the researcher deems the presence of such a staff member as not just a recommendation, but rather a requirement. Such members of staff should be tasked with the creation of security incident response procedures as well as communicating with the relevant cloud providers. Levels of transparency

should be established at not just the cloud provider's side, but also the university's side. This would entail the sharing of information that might directly affect the users, such as disclosing breaches in security. If no awareness campaigns have been conducted and the user base is uneducated such forms of disclosure could be counter productive, hence the need to educate and make users aware of cloud security.

- **Rate the criticality and suitability of information:** The interview data indicated that not all key stakeholders agree on the criticality of certain types of information. For this reason it is vital to also consider for what type of data the cloud will be utilized and the impact it might have on the daily operation of the university. Some participants indicated that email could easily be located in the cloud, since not being able to access it for several hours is not a major concern. The same could not be said of financial systems or anything related to teaching, since these are deemed critical systems. Rating the criticality and suitability of information in this way should be regarded as a first step towards adopting the cloud.

- **Perform a threat assessment:** Many key stakeholders were not aware of the specific threats to a cloud infrastructure. This highlights the need to not only become familiar with these threats, but to also identify the likelihood of them occurring within the operational context of their universities. In the South African context SANReN is seen as a cloud enabler and for this reason the impact of network outages needs to be explored. Measures need to taken to address internal threats, since most of the participants regard this as a concern.

- **Collaborate with other universities:** Many participants explicitly stated that the competitiveness amongst South African universities is counter productive and that many problems (not limited to cloud adoption) can be addressed if South African universities work together. Some participants even hinted at the notion to establish shared data centres, which could act as community clouds. This would save costs in the long term, not only on hardware and software, but also on salaries since the same staff members could effectively service multiple universities. Some participants felt that TENET should act as the pioneers in this regard.

Although these recommendations are aimed at a higher level, South African universities would be wise to investigate them further before starting a cloud adoption campaign. The researcher anticipates that such investigations will allow future researchers to break these recommendations up into even more detailed components. Some additional areas of future research is listed in the following section.

5.6 Future Research

During this study a number of additional areas of research emerged. It is the researchers' belief that these areas of research will not only further some of the contributions made by this study, but also allow for the exploration of cloud computing in ways which could add to this list of contributions.

With a very specific focus on certain South African universities this study could be expanded to include all South African universities. Using Skype[1] (as one component of a research instrument) researchers could do a comparative study with universities in other developing countries. This could then be contrasted with the views of university key stakeholders in developed countries. The views of key stakeholders in the private sector could also be contrasted with the views of university key stakeholders. Another useful study would be to gain insight into the views of cloud providers. Findings from the aforementioned studies will not only allow for some new contributions, but also give the industry and researchers a complete overview as to what are the views of key stakeholders.

The physical location of data is also an area of concern. Many of the key stakeholders in this study raised concerns about the legal implications this has for universities which are making use of cloud providers with data centres in other jurisdictional areas. Further research around the legal implications of this could yield results useful to cloud providers and subscribers. In line with such legal studies it would also be useful to gather some in-depth views on what cloud subscribers think they are receiving when they sign up for cloud service as opposed to what they are actually getting. This pertains specifically to the terms of service.

With so many participants viewing SANReN as a cloud enabler it would make sense to also study how it has influenced the use of cloud services since its inception. If possible, even indicating how the adoption and use of cloud services has changed over this period of time.

From the results presented in *Chapter Four* the importance of trust is evident, especially with it being depicted as a main theme on the thematic map (see *Figure 4.5*) as well as a core concept on the new conceptual framework illustrated in *Figure 4.6*. For this reason further research on the views of key stakeholders with regard to the concept of trust could be useful. One such area of research is the views key stakeholders have with regard to trust brokers in the cloud. Results of such studies could be used by trust brokers to enhance their services and perhaps tailor cloud services, depending on the sector within which a prospective client operates.

The researcher anticipates that all of the possible studies listed above will benefit the field of cloud computing, but suggests that an in-depth (qualitative) approach be used in the exploration of these topics. It was the qualitative

[1] www.skype.com

and interpretive nature of this study that enabled the researcher to identify these areas of future research. In many instances it was the context surrounding a specific interpretation that indicated this to the researcher. This does not preclude the use of surveys and other positivist methods to gain insight into these areas of future research.

5.7 Limitations Revisited

Before concluding the researcher would like to recognise some of the limitations of this study. First and foremost, this study only focused on specific key stakeholders within a few South African universities. These key stakeholders were limited to IT professionals and did not include any participants from academia. For this reason the views expressed in this study are to be seen in an operational light, with very few, if any, consideration of the challenges faced by academic departments. Although every effort was made to generalize the recommendations (see *Section 5.5*) made earlier the researcher cannot ignore the contextual influences that gave rise to these recommendations.

More specific limitations apply to the online survey, since it was only presented in English and did not include any other official South African languages. Economic limitations also applied in that the researcher was not able to travel to more South African universities. Some participants did not have a strong technical background which limited their responses with regard to technical cloud computing threats.

The context sensitive nature of this study also limits the generalizability of its results and interpretations. Not only are the interpretations not generalizable, but they are also dependent on the operational context and background of the researcher.

5.8 Summary of Dissertation

Although this study has addressed some aspects of the research areas listed above, it has formed only one part of a larger study on cloud information security. In *Chapter One* the researcher gave an overview of how the cloud is currently being used by some universities, highlighting specific problems pertaining to universities in South Africa. This process culminated with the researcher formally stating the research questions (see *Section 1.2*) and briefly discussed the methodology that was used to answer these questions. *Chapter One* concluded with the limitations of this study as well as a brief outline of this dissertation.

In *Chapter Two* the reader was given an overview of cloud computing making sure to include the necessary theoretical background on the various components of the research questions. In this review of the literature both general and specific topics were discussed, with the researcher paying specific attention to topics, such as cloud computing threats (see *Section 2.5 and 2.6*) and security incident response in the cloud (see *Section 2.7*). The core concepts of the literature review were summarized by presenting the reader with a conceptual framework (see *Section 2.9*) illustrating the researchers' understanding of how these concepts are related. In essence *Chapter Two* provided this study with a theoretical lens upon which the survey and interview questions were based.

The brief methodological discussion in *Chapter One* now gave way to a detailed discussion of how the researcher intended on collecting, analysing and interpreting the research data. For this reason *Chapter Three* discussed several key research design elements. These elements not only included the chosen paradigm and associated research methods, but also detailed discussions on the process of data collection and analysis. Specific attention was given to not only the data collection instruments and the questions of which they were comprised, but also the purpose of each interview question and how they addressed the research questions. A detailed discussion on the method of analysis (thematic analysis) and the six phases it is comprised of concluded *Chapter Three*.

In *Chapter Four* the results of the online survey as well as the analysis and interpretation of the interview data was discussed. The chapter started with a discussion on the results of the online survey by illustrating some graphs around the research questions of this study. The process of analysis was demonstrated by progression through each of the six phases ensuring the inclusion of actual extracts of the coding frameworks. This process concluded with a complete illustration of the final thematic map. It is only after this that the actual process of interpretation (via a cross case narrative) took place. Using this final thematic map (*Figure 4.5*) and a new conceptual framework (*Figure 4.6*) interpretation of the interview data occurred ensuring specific reference to the context within which these interpretations was made. For this reason *Chapter Four* formed a core component of this thesis, since it is in this chapter that the research questions were addressed.

This chapter has for the most part served as a summary of what this dissertation set out to achieve as well as how this was achieved. Not only did the researcher make specific reference to the contributions of this study, but also provided some recommendations for South African universities. The chapter also indicated how further research could benefit the field of cloud computing. Importantly, *Chapter Five* provided an explanation as to how the research questions have been addressed as well as the limitations of this study's results and interpretations.

5.9 Conclusion

This study has demonstrated just how complex key stakeholder views are when considering the security of cloud-based information. It has also demonstrated that there is some merit in using a qualitative approach to a topic often explored in a technical manner. This stems mainly from the fact that the main proponent, adopter and user of the cloud is indeed a human; a human not only subject to the technical aspects of the cloud, but also the context within this cloud is to be utilized.

References

[1] Appirio. State of the Public Cloud: The Cloud Adopters' Perspective. Online. Available from: `http://thecloud.appirio.com/rs/appirio/images/State_of_the_Public_Cloud_Results_FINAL-102910.pdf`, Last Accessed: 13 August 2013.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. A View of Cloud Computing. *Communications of the ACM, 53 (4)*, 50–58.

[3] Attride-Stirling, J. Thematic Networks: An Analytic Tool for Qualitative Research. *Qualitative Research, 1 (3)*, 385–405.

[4] Basta, A., and Halton, W. *Computer Security and Penetration Testing.* Cengage Learning, Stamford, 2007.

[5] Baxter, P., and Jack, S. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report, 13 (4)*, 544–559.

[6] Behrend, T. S., Wiebe, E. N., London, J. E., and Johnson, E. C. Cloud Computing Adoption and Usage in Community Colleges. *Behaviour & Information Technology, 30 (2)*, 231–240.

[7] Bird, C. M. How I Stopped Dreading and Learned to Love Transcription. *Qualitative Inquiry, 11 (2)*, 226–248.

[8] Bowers, K. D., Juels, A., and Oprea, A. HAIL: A High-Availability and Integrity Layer for Cloud Storage. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (New York, USA, 2009), ACM, 187–198.

[9] Bradshaw, S., Millard, C., and Walden, I. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *International Journal of Law and Information Technology, 19 (3)*, 187–223.

[10] Braun, V., and Clarke, V. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology, 3 (2)*, 77–101.

[11] Bryman, A. *Social Research Methods.* Oxford University Press, New York, 2012.

[12] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. *Future Generation Computer Systems, 25 (6)*, 599–616.

[13] Cachin, C., Keidar, I., and Shraer, A. Trusting the Cloud. *SIGACT News, 40 (2)*, 81–86.

[14] Centre for Higher Education Transformation. Institutional Clusters in Higher Education in South Africa. Online. Available from: `http://chet.org.za/files/DifferentiationChet_Web10May10.pdf`, Last Accessed: 13 August 2013.

[15] Chen, Y., and Sion, R. On Securing Untrusted Clouds with Cryptography. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (New York, USA, 2010), ACM, 109–114.

[16] Choubey, R., Dubey, R., and Bhattacharjee, J. A Survey on Cloud Computing Security, Challenges and Threats. *International Journal on Computer Science and Engineering, 3 (3)*, 1227–1231.

[17] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., and Molina, J. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security* (New York, USA, 2009), ACM, 85–90.

[18] Cisco Systems. Cloud 101: Developing a Cloud Computing Strategy for Higher Education. Online. Available from: `http://www.cisco.com/en/US/services/collateral/ps10658/ps11785/cloud_101_higher_education_wp.pdf`, Last Accessed: 13 August 2013.

[19] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Online. Available from: `https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf`, Last Accessed: 13 August 2013.

[20] Cloud Security Alliance. Top Threats to Cloud Computing v1.0. Online. Available from: `https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf`, Last Accessed: 13 August 2013.

[21] Cole, M., and Avison, D. The Potential of Hermeneutics in Information Systems Research. *European Journal of Information Systems, 16 (6)*, 820–833.

[22] Couper, M. P., Traugott, M. W., and Lamias, M. J. Web Survey Design and Administration. *Public Opinion Quarterly, 65 (2)*, 230–253.

[23] Creeger, M. Cloud Computing: An Overview. *ACM Queue, 7 (5)*, 3–4.

[24] Dahbur, K., Mohammad, B., and Tarakji, A. B. A Survey of Risks, Threats and Vulnerabilities in Cloud Computing. In *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications* (New York, USA, 2011), ACM, 1–6.

[25] Data Security Council of India. Data Protection Challenges in Cloud Computing: An Indian Perspective. Online. Available from: http://www.dsci.in/sites/default/files/Data%20Protection%20Challenges%20in%20Cloud%20Computing.pdf, Last Accessed: 13 August 2013.

[26] Dawoud, W., Takouna, I., and Meinel, C. Infrastructure as a Service Security: Challenges and Solutions. In *Proceedings of the 7th International Conference on Informatics and Systems* (Cairo, Egypt, 2010), IEEE, 1–8.

[27] Deloitte. Cloud Adoption Study: Cloud Computing is Gaining Momentum. Online. Available from: http://www.deloitte.com/assets/Dcom-Belgium/Local%20Assets/Documents/EN/Services/Consulting/dcom-be-en-cloud-adoption-survey.pdf, Last Accessed: 13 August 2013.

[28] DiCicco-Bloom, B., and Crabtree, B. F. The Qualitative Research Interview. *Medical Education, 40 (4)*, 314–321.

[29] Dillman, D. A., Smyth, J. D., and Christian, L. M. *Internet, Mail and Mixed-mode Surveys: The Tailored Design Method*. Wiley, New Jersey, 2009.

[30] Dillon, T., Wu, C., and Chang, E. Cloud Computing: Issues and Challenges. In *Proceedings of the 24th International Conference on Advanced Information Networking and Applications* (Perth, Australia, 2010), IEEE, 27–33.

[31] Durkee, D. Why Cloud Computing Will Never Be Free. *ACM Queue, 8 (4)*, 20–29.

[32] Elliott, R., Fischer, C. T., and Rennie, D. L. Evolving Guidelines for Publication of Qualitative Research Studies in Psychology and Related Fields. *British Journal of Clinical Psychology, 38 (3)*, 215–229.

[33] Erenben, C. Cloud Computing: The Economic Imperitive. Online. Available from: http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GENPRESS/E090302E.pdf, Last Accessed: 13 August 2013.

[34] European Network and Information Security Agency. Cloud Computing: Benefits, Risks and Recommendations for Information Security. Online. Available from: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file, Last Accessed: 13 August 2013.

[35] Executive Brief. The Pros and Cons of SaaS - Part 2. Online. Available from: http://www.executivebrief.com/blogs/the-pros-and-cons-of-saas-part-2/, Last Accessed: 13 August 2013.

[36] f5 Networks. Cloud Computing Survey Results. Online. Available from: `http://www.f5.com/pdf/reports/cloud-computing-survey-results-2009.pdf`, Last Accessed: 13 August 2013.

[37] Farrell, R. Securing the Cloud: Governance, Risk, and Compliance Issues Reign Supreme. *Information Security Journal: A Global Perspective, 19 (6)*, 310–319.

[38] Fereday, J., and Muir-Cochrane, E. Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods, 5 (1)*, 80–92.

[39] Genesis Analytics Pty (Ltd). Telecommunications Prices in South Africa: An International Peer Group Comparison. Online. Available from: `http://thornton.co.za/resources/12568Telecomm_web.pdf`, Last Acessed: 13 August 2013.

[40] Gillwald, A. Between Two Stools: Broadband Policy in South Africa. *The South African Journal of Information and Communication, 1 (8)*, 53–77.

[41] Gillwald, A. Good Intentions, Poor Outcomes: Telecommunications Reform in South Africa. *Telecommunications Policy, 29 (7)*, 469–491.

[42] Grobauer, B., and Schreck, T. Towards Incident Handling in the Cloud: Challenges and Approaches. In *Proceedings of the 2010 ACM Workshop on Cloud Computing Security* (New York, USA, 2010), ACM, 77–86.

[43] Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., Feldman, A. J., Appelbaum, J., and Felten, E. W. Lest We Remember: Cold-boot Attacks on Encryption Keys. *Communications of the ACM, 52 (5)*, 91–98.

[44] Harauz, L. M. K., and Potter, B. Data Security in the World of Cloud Computing. *Security and Privacy, 7 (4)*, 61–64.

[45] Heerwegh, D. An Investigation of the Effect of Lotteries on Web Survey Response Rates. *Field Methods, 18 (2)*, 205–220.

[46] Holstein, J., and Gubrium, J. *Phenomenology, Ethnomethodology and Interpretive Practice.* in Denzin, N., Lincoln, Y. ed. Handbook of Qualitative Research, Sage Publications, 1994, 262–272.

[47] Ion, I., Sachdeva, N., Kumaraguru, P., and Čapkun, S. Home is Safer than the Cloud!: Privacy Concerns for Consumer Cloud Storage. In *Proceedings of the 7th Symposium on Usable Privacy and Security* (New York, USA, 2011), ACM, 1–20.

[48] Jaeger, P. T., Lin, J., and Grimes, J. M. Cloud Computing and Information Policy: Computing in a Policy Cloud? *Journal of Information Technology & Politics, 5 (3)*, 269–283.

[49] Joint, A., Baker, E., and Eccles, E. Hey, You, Get Off of That Cloud? *Computer Law & Security Review, 25 (3)*, 270–274.

[50] Khorshed, M. T., Ali, A. S., and Wasimi, S. A. A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing. *Future Generation Computer Systems, 28 (6)*, 833–851.

[51] Kim, W., Kim, S. D., Lee, E., and Lee, S. Adoption Issues for Cloud Computing. In *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia* (New York, USA, 2009), ACM, 2–5.

[52] King, N., and Horrocks, C. *Interviews in Qualitative Research.* Sage Publications, New York, 2010.

[53] Klein, H. K., and Myers, M. D. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly, 23 (1)*, 67–93.

[54] Kroeze, J. *Postmodernism, Interpretivism, and Formal Ontologies.* in Mora, M., Gelman, O., Steenkamp, A. and Raisinghani, M.S. ed. Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems, Hershey: IGI Global, 2012, 43–62.

[55] Kumar, P., Sehgal, V. K., Chauhan, D. S., Gupta, P. K., and Diwakar, M. Effective Ways of Secure, Private and Trusted Cloud Computing. *International Journal of Computer Science Issues, 8 (3)*, 412–421.

[56] Lin, A. C. Bridging Positivist and Interpretivist Approaches to Qualitative Methods. *Policy Studies Journal, 26 (1)*, 162–180.

[57] MacGregor, K. South Africa: New University Clusters Emerge. Online. Available from: `http://www.universityworldnews.com/article.php?story=20100523104119724`, Last Accessed: 13 August 2013.

[58] Mack, L. The Philosophical Underpinnings of Educational Research. *Polyglossia, 19*, 5–11.

[59] Molnar, D., and Schechter, S. Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In *Proceedings of the 9th Workshop on the Economics of Information Security* (Cambridge, USA, 2010), Microsoft Research, 1–18.

[60] Monfared, A. T. Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments. Online. Available from: `http://www.cse.hut.fi/en/publications/B/11/papers/taheri.pdf`, Last Accessed: 13 August 2013.

[61] Morgan, G., and Smircich, L. The Case for Qualitative Research. *The Academy of Management Review, 5 (4)*, 491–500.

[62] Myers, M. D., and Newman, M. The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization, 17 (1)*, 2–26.

[63] National Institute of Standards and Technology. Computer Security Incident Handling Guide. Online. Available from: `http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf`, Last Accessed: 13 August 2013.

[64] National Institute of Standards and Technology. Guidelines on Security and Privacy in Public Cloud Computing. Online. Available from: `http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf`, Last Accessed: 13 August 2013.

[65] Nelson, M. R. The Cloud, the Crowd, and Public Policy. *Issues in Science & Technology, 25 (4)*, 71.

[66] Okuhara, M., Shiozaki, T., and Suzuki, T. Security Architectures for Cloud Computing. *FUJITSU Scientific and Technical Journal, 46 (4)*, 397–402.

[67] Patton, M. *Qualitative evaluation and research methods*. Sage Publications, New York, 1990.

[68] Ponemon Institute. Security of Cloud Computing Users: A Study of Practitioners in the US & Europe. Online. Available from: `http://www.ca.com/us/~/media/files/industryresearch/security-cloud-computing-users_235659.aspx`, Last Accessed: 13 August 2013.

[69] PriceWaterhouseCoopers. Trial by Fire. Online. Available from: `http://www.pwc.com/en_US/us/it-risk-security/assets/trial-by-fire.pdf`, Last Accessed: 13 August 2013.

[70] Puttaswamy, K. P. N., Kruegel, C., and Zhao, B. Y. Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications. In *Proceedings of the 2nd ACM Symposium on Cloud Computing* (New York, USA, 2011), ACM, 1–13.

[71] Ramgovind, S., Eloff, M., and Smith, E. The Management of Security in Cloud Computing. In *Proceedings of the 2010 Information Security for South Africa Conference* (Johannesburg, South Africa, 2010), IEEE, 1–7.

[72] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (New York, USA, 2009), ACM, 199–212.

[73] Roberts, II, J. C., and Al-Hamdani, W. Who can You Trust in the Cloud?: A Review of Security Issues within Cloud Computing. In *Proceedings of the 2011 Information Security Curriculum Development Conference* (New York, USA, 2011), ACM, 15–19.

[74] SANReN. Overview. Online. Available from: `http://www.sanren.ac.za/overview`, Last Accessed: 13 August 2013.

[75] SANS Institute. Following Incidents Into the Cloud. Online. Available from: `http://www.sans.org/reading_room/whitepapers/incident/incidents-cloud_33619`, Last Accessed: 13 August 2013.

[76] Saripalli, P., and Walters, B. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In *Proceedings of the 3rd International Conference on Cloud Computing* (Miami, USA, 2010), IEEE, 280–288.

[77] Schaffer, H. E., Averitt, S. F., Hoit, M. I., Peeler, A., Sills, E. D., and Vouk, M. A. NCSU's Virtual Computing Lab: A Cloud Computing Solution. *Computer, 42 (7)*, 94–97.

[78] Schostak, J. *Interviewing and Representation in Qualitative Research*. McGraw-Hill International, 2006.

[79] Schutz, A. *The Phenomenology of the Social World*. Northwestern University Press, 1967.

[80] Schutz, A. *Collected Papers: The Problem of Social Reality*. Kluwer Academic Publications, 1982.

[81] Schutz, A. *Alfred Schutz on Phenomenology and Social Relations*. University of Chicago Press, 1999.

[82] Shin, S., and Kobara, K. Towards Secure Cloud Storage. Online. Available from: `http://salsahpc.indiana.edu/CloudCom2010/Edemo/Towards%20Secure%20Cloud%20Storage.pdf`, Last Accessed: 13 August 2013.

[83] Simons, H. *Case Study Research in Practise*. Sage Publications, New York, 2009.

[84] Subashini, S., and Kavitha, V. A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications, 34 (1)*, 1–11.

[85] SurveyMonkey. Smart Survey Design. Online. Available from: `http://s3.amazonaws.com/SurveyMonkeyFiles/SmartSurvey.pdf`, Last Accessed: 13 August 2013.

[86] Suzaki, K., Iijima, K., Yagi, T., and Artho, C. Memory Deduplication as a Threat to the Guest OS. In *Proceedings of the 4th European Workshop on System Security* (New York, USA, 2011), ACM, 1–6.

[87] Szefer, J., and Lee, R. B. Architectural Support for Hypervisor-Secure Virtualization. *ACM SIGARCH Computer Architecture News, 40 (1)*, 437–450.

[88] Tout, S., Sverdlik, W., and Lawver, G. Cloud Computing and its Security in Higher Education. In *Proceedings of the 2009 Information Systems Education Conference* (Washington, USA, 2009), EDSIG, 1–5.

[89] Travis, J. Exploring the Constructs of Evaluative Criteria for Interpretivist Research. In *Proceedings of the 10th Australasian Conference on Information Systems* (Wellington, New Zealand, 1999), Citeseer, 1037–1049.

[90] Walsham, G. The Emergence of Interpretivism in IS Research. *Information Systems Research, 6 (4)*, 376–394.

[91] Walsham, G. *Interpreting Information Systems in Organizations*. Wiley, New Jersey, 1993.

[92] Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D., and Karl, W. Scientific Cloud Computing: Early Definition and Experience. In *Proceedings of the 10th International Conference on High Performance Computing and Communications* (Dalian, China, 2008), IEEE, 825–830.

[93] Wei, J., Zhang, X., Ammons, G., Bala, V., and Ning, P. Managing Security of Virtual Machine Images in a Cloud Environment. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security* (New York, USA, 2009), ACM, 91–96.

[94] Wrenn, G. Unisys Secure Cloud: Addressing the Top Threats of Cloud Computing. Online. Available from: `http://downloads.sys-con.com/download/whitepaper_unisys_padlock`, Last Accessed: 13 August 2013.

[95] Xiong, H., Zhang, X., Yao, D., Wu, X., and Wen, Y. Towards End-To-End Secure Content Storage and Delivery with Public Cloud. In *Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy* (New York, USA, 2012), ACM, 257–266.

[96] Yanow, D., and Schwartz-Shea, P. *Interpretive Research Design: Concepts and Processes*. Routledge, New York, 2012.

[97] Yin, R. K. The Case Study Crisis: Some Answers. *Administrative Science Quarterly, 26 (1)*, 58–65.

[98] Zissis, D., and Lekkas, D. Addressing Cloud Computing Security Issues. *Future Generation Computer Systems, 28 (3)*, 583–592.