KNOWLEDGE SECURITY
How Do Organizations Model or Conduct Knowledge Security in order to secure their Knowledge Assets to their Optimal Benefits?

Banyatsang Mphago

Master program
Master of Science in Information Security

Luleå University of Technology
Department of Computer science, Electrical and Space Engineering
Acknowledgements

Tough times came and now they are gone. Finally, after two years of hard work since the start of my master thesis, the dream of seeing myself as an information security professional become more a reality. Challenges throughout my research process and even throughout my entire master programme came in large numbers, and I would like to express my greatest gratitude for myself for never being deterred by such challenges until the end of the programme. If not because of the support of my two lovely supervisors, Prof. Dan Harnesk and Dr. Hugo Quisbert, this document I call my master thesis would have never came to being, and I would like to thank them very much for the unquestionable support and guidance they gave me throughout my entire research. Most importantly, I would like to thank LTU for giving me the opportunity to realise my dream, and all everyone, not forgetting all LTU lectures that helped me throughout my time with the university.

I would also like to thank my one year old son, Tumo, for giving me extra energy to excel with studies and being the reason of my sleepless hard work I showed throughout my study, and not forgetting his mom for always pushing me to do more. It will be the biggest mistake to forget to thank all the organisations that helped me in conducting my researches with them until the end of the programme. In the end I would thank everyone who wished me well with my studies, and most notably, Kamogelo Puleng, for giving me the light on how to go about with my studies.

THANK YOU!!!!!!!!!!!!!!!

Mphago Banyatsang
Abstract

The security of knowledge is of extreme importance to any organisation, as organisations are increasingly becoming dependent on knowledge assets as a primary source of competitive advantage. However, most organisations have not yet realised the importance of securing these knowledge assets. Despite the fact that knowledge is a public good when shared among others, knowledge assets lose their competitiveness when accessible to un-authorised individuals. This paper is seeking to explore how organisations around Botswana secure their knowledge assets, and by doing so, it categorises knowledge security into three levels; the product, the people, and the process. The product seeks to find how codified knowledge is secured, the process seeks to find how the process of knowledge generation is secured, and people seek to find how organisations handle employees in order to secure knowledge assets. At the end, the paper provides some recommendations/or framework that the organisations can use to better secure their knowledge assets.
# TABLE OF CONTENTS

Acknowledgements .................................................................................................................. 1  
Abstract ................................................................................................................................... 2  
LIST OF FIGURES ..................................................................................................................... 5  
LIST OF TABLES ....................................................................................................................... 5  
CHAPTER 1 .................................................................................................................................... 7  
  1. INTRODUCTION .................................................................................................................. 7  
     1.1 Background ........................................................................................................................... 7  
     1.2 Problem Description .......................................................................................................... 10  
     1.3 Research Objectives ......................................................................................................... 11  
     1.4 Research Question ............................................................................................................ 12  
     1.5 Research Delimitations .................................................................................................... 12  
CHAPTER 2 .................................................................................................................................... 13  
  2. LITERATURE REVIEW ......................................................................................................... 13  
     2.1 What is Data? ..................................................................................................................... 13  
     2.2 What is Information? ........................................................................................................ 14  
     2.3 What is knowledge? ......................................................................................................... 15  
        2.3.1 Tacit Knowledge ......................................................................................................... 16  
        2.3.2 Explicit Knowledge ................................................................................................. 17  
        2.3.3 Knowledge Assets ................................................................................................. 17  
     2.4 What is Organisational Knowledge? ................................................................................ 19  
     2.5 What is Optimal Benefits? .............................................................................................. 20  
     2.6 Strategic Considerations in securing Knowledge Assets ................................................. 20  
     2.7 Identifying Intellectual Assets .......................................................................................... 23  
CHAPTER 3 .................................................................................................................................... 26
3. THEORATICAL FRAMEWORK ................................................................. 26
3.1 Knowledge the Product, Process and People ........................................ 26
3.2 Knowledge and the Theory of the Firm .................................................. 28
3.3 Securing Knowledge Assets and Processes; Lessons from Defence and Intelligence Sectors 31
3.4 Theory of Organizational Knowledge Creation ...................................... 35
  3.4.1 The Two Dimensions of Knowledge Creation .................................. 36
  3.4.2 Conversion/Interaction of Tacit Knowledge to Explicit Knowledge .......... 37
  3.4.3 Socialization (Tacit to Tacit) ............................................................ 38
  3.4.4 Externalisation (Tacit to Explicit) ..................................................... 38
  3.4.5 Combination (Explicit to Explicit) ................................................... 39
  3.4.6 Internalization (Explicit to Tacit) .................................................... 39
3.5 Security Awareness and Training ............................................................. 40
  3.5.1 The Continuum .............................................................................. 42
  3.5.2 Who does what? ........................................................................... 43
3.6 The Incentive Theory of Motivation ....................................................... 44

CHAPTER 4 ....................................................................................................... 46
4. METHODOLOGY .......................................................................................... 46
  4.1 Research Purpose .................................................................................. 46
  4.2 Research Approach .............................................................................. 46
  4.3 Research Strategy ................................................................................ 47
  4.4 Data Collection Method ...................................................................... 48
  4.5 Analysis Plan ....................................................................................... 49

CHAPTER 5 ....................................................................................................... 50
5. EMPERICAL SETTINGS AND DATA .......................................................... 50
5.1 University of Botswana (UB) ................................................................. 50
5.2 Ministry of Health (MoH)................................................................. 53
5.3 HiPerformance Systems Botswana (HPS) ........................................... 55
5.4 Department of Water Affairs (DWA) .................................................. 57
5.5 Air Botswana (AB) .............................................................................. 60

CHAPTER 6 ......................................................................................... 62
6. RESULTS ANALYSIS ........................................................................... 62
   6.1 On the Knowledge Security Categories and Content ......................... 62

CHAPTER 7 ......................................................................................... 70
7.1 DISCUSSIONS AND CONCLUSIONS .............................................. 70
7.2 RECOMMENDATIONS ....................................................................... 75

FURTHER STUDIES .............................................................................. 86
REFERENCES ......................................................................................... 87
APPENDICES .......................................................................................... 92

LIST OF FIGURES
Figure 1: the seven strategic considerations (Desouza, 2007) ....................... 20
Figure 2: Two Dimensions of Knowledge Creation (Nonaka & Takeuchi, 1995) .................................................. 36
Figure 3; Four Modes of Knowledge Conversion (Nonaka & Takeuchi, 1995) .................................................. 38
Figure 5. Summary of Proposed Framework ................................................ 85

LIST OF TABLES
Table 1 Data Coding and Interpretations .................................................... 62
Table 2 Emerged Data Patterns ................................................................ 65
CHAPTER 1

1. INTRODUCTION

Knowledge security is an emerging field of research area which focuses on the protection of knowledge assets within organisations. My focus on this research is, based on the problematic nature of protecting knowledge assets, how do organisations overcome such problems and effectively protect their knowledge assets in order to keep the competitive advantage over the rest.

1.1 Background

Organizations are increasingly becoming dependent on knowledge assets as a primary source of competitive advantage. Knowledge management typically, aims at increasing the transparency of knowledge, codifying it and enhancing knowledge sharing in order to improve reuse of knowledge assets. But knowledge assets do not hold that competitive advantage if they are accessible to unauthorised individuals. Just like information, knowledge needs to be secured and only be accessible to the authorised individuals. (Desouza, 2007), stated that “organizational knowledge resources are proprietary to the organization. To keep them proprietary we must keep them secure from un-authorised use, tampering, acts of vandalism, and sabotage.” Knowledge based assets and knowledge based processes are the sources of competitive advantages for organizations. They are the drivers behind usage of other resources and they are often very hard, if not possible to substitute. If they go missing or if they lose their value, the organization will have to use lower quality resources to cover up.

(Desouza, 2007), stated that an organization is differentiated by the knowledge it possesses, and how it employs that knowledge to further its business agenda. Loose this knowledge, or misuse it, and the organization may face disastrous consequences. Most organizations do not know how to secure their intellectual assets, more precisely, during crisis. As such, they lose their most valuable assets during most time of vulnerability. Take for example; an organization is losing employees in one of its most critical department, information security. How is the organization supposed to recover this departing knowledge? It’s not all about hiring new staff. The new staffs lack critical knowledge that the departing staff holds. Knew staff need to take some time to learn their new environment, and some of the concepts may never be understood at all without the departed staff.
(Desouza & Vanapalli, 2005), also stated that Knowledge resources are the source of competitive advantage for organizations, unless we have apt security measures in place, we risk losing them to acts of theft, misuse, espionage, and disasters. Unless we know how to secure our knowledge assets, knowing how to manage them plays a very insignificant role in making organisations competitive over the rest. Take for example, the Coca-Cola Company. If their methods and processes of brewing coke leaks to the competitors, will coke still make those headlines in terms of its sales? Of course those competitors will try to improve on top of Coca-Cola processes with the knowledge they already have, and surpass coke sales. So, what is the best way to protect your knowledge and let no one use it to overpower you?

Securing knowledge assets generally is a very challenging task. Many organizations don’t realise that, the most secure and impenetrable defences are useless if they cover only a portion of what need to be protected. They don’t realise that protecting cooperate knowledge has more to do with people than it does guards and technology. (Desouza, 2007), stated that most organizations lack significant programmes to secure their knowledge assets, and the only real security a man can have in this world is a reserve of knowledge, experience and ability. While organizations are spending a great deal of effort, time and resources in creating their knowledge assets, they are not spending commensurate efforts on protecting these efforts. Organizations don’t even know what their most valuable intellectual assets are, and furthermore, they lack an appreciation for the fact that these assets need to be secured and protected so as to preserve and extend the competitive advantage. It is common to find organizations that think asking someone to sign a non-disclosure agreement are enough to prevent knowledge leakage. Such thinking is not only naïve but can cost an organization is own existence, says (Desouza, 2007).

(Liebeskind, 1996), stated that knowledge about a manufacturing technology or a new product in development is accessible to the workers and managers involved, while final products can be observed by any buyer, and in addition, knowledge is a public good; one item of knowledge can be used by many individuals or organisations at the same time, without diminishing its productivity for any one user. In other words, illegal use of knowledge can be very difficult and costly to detect. (Liebeskind, 1996), stated that the fact that knowledge is more easily expropriated and imitated than other types of assets is not a problem when it can be generated and commercialized by a single person. However, in many instances, producing valuable knowledge will require the input of proprietary, personal knowledge from a number of different individuals, each of whom must exchange some of her knowledge with other team members. In this case, if one member of a
knowledge production team can obtain and absorb the knowledge of other team members, she has an incentive to expropriate that knowledge for her own use or to leak it to competitors, eliminating the monopoly on that knowledge that the team might otherwise possess.

Security of cooperate assets is more complex as knowledge becomes a key organizational resource, says (Neville, Powell, & Panteli, 2003), and traditionally, security has been concerned with the protection of assets. Valuable information has always been guarded in order to retain its worth and provide advantage over a competitor. The increasing value of knowledge means that the complexity of security solutions needed to guard corporate secrets has increased. (Whitman & Mattord, 2009), defines security as the quality or state of being secure- to be free from danger. In other words, protection against adversaries— from those who would do harm, intentionally or otherwise— is the objective. On that logical aspect, knowledge security would be the quality or state of being secure, or being free from danger of knowledge assets. Knowledge security as a concept, would deal with the protection of knowledge assets in a firm.

(Neville, Powell, & Panteli, 2003), stated that the first step in securing knowledge is to examine potential threats from the internal and external environment. Once threats have been identified, resources are needed to combat them— risk management and evaluation; though a successful security policy needs to be pro-active. (French, 2007) finds the value of knowledge to an organization as supported with the growing support and implementation of knowledge management systems. She states that security of organizational knowledge is a multi–faceted challenge. Organizations need to incorporate reliable and cost–effective security measures to protect organizational knowledge from destruction or loss as well as unauthorised access or modifications.

According to (Liebeskind, 1996), firms as institutions, play a critical role in creating and sustaining a competitive advantage; that of protecting valuable knowledge. Specifically, because property rights in knowledge are weak, and are costly to write and enforce, firms are able to use an array of organisational arrangements that are not available in markets to protect the value of knowledge. Thus, firms can differentially prevent expropriation of knowledge and differentially reduce the observability of knowledge and its products, thereby protecting against imitation (Liebeskind, 1996). In this way, firms are able to create possession rights to knowledge that are just as valuable, if not more valuable, than the limited property rights to knowledge accorded under the law. This argument have
important implications that suggest that the condition of uniqueness that is so central to the strategy theory depends critically upon the deployment of protective organisational arrangements by firms. Thus, the organisation of a firm can serve as an important, if not critical, isolating mechanism. Consequently, considering the fact that resources and capabilities are distributed asymmetrically across firms may be attributed not only to luck, success in search, history or inherent causal ambiguity, but also to the fact that some firms are able to protect their knowledge from expropriation and imitation more effectively than other firms (Liebeskind, 1996).

(Liebeskind, 1996), also stated that considering firms as institutions that are able to protect the value of knowledge provides a direct connection between the organisational characteristics of the firms on the one hand, and their dynamic strategic behaviour on the other. (Liebeskind, 1996), argued that by protecting knowledge, firms may serve to induce investment in strategic innovation, because the incentives to innovate depend on the degree to which the innovator can appropriate future rent streams, and in addition, if some firms are able to protect the value of their knowledge more effectively than other firms, these firms will have more high powered incentives to innovate. Thus, we should expect to observe a long-run correlation between a firm’s rate of innovation and its success in protecting the knowledge that it generates.

1.2 Problem Description

The practices and literature of knowledge management tells us that knowledge should be shared and made available to all, as it is a social good that grows when shared and combined with the experience of others. But then, knowledge is not like a physical product, which can be tagged and inventoried for everyone to see that it is protected and belongs to someone else (Desouza, 2007). Knowledge resides in the minds of employees, embedded in work processes, and is captured in product and service offerings.

This typically makes the protection of knowledge assets a very daunting task. For example, (Desouza, 2006), stated that knowledge residing in organizations is difficult to visualize. Then, if knowledge cannot be visualised, how is it protected? Secondly, he stated that unlike information, knowledge is fluid, dynamic and more mobile than information, and it
changes its state as it is exchanged between individuals and entities. The fluidity, dynamism, and mobility of knowledge make it more difficult to pin down and capture, hence difficult to protect.

The problematic nature of securing knowledge assets is also perceived by (Liebeskind, 1996). Among this problems are the extreme limitations of property rights in protecting knowledge. (Liebeskind, 1996), stated that property rights in knowledge such as patents, copyrights, and trade secrets, are very narrowly defined under the law, and are costly to write and enforce. Patents are published, and so reveal the knowledge of the firm to its rivals. Patents are only issued after a costly proving process, and can be challenged by other parties, and even overturned. Copyrights creates ownership rights only for a certain encoded products such as written documents, music, artwork, films, photographs, software, and technical drawings. Copyrights also have a limited life, and are costly to enforce because the plaintiff have to prove novelty of their copyrighted product for any suit for infringement to be successful. Trade secrets laws apply only to knowledge that is codified and is in continuous use; non continuous knowledge such as contract bids, plans or prototypes, and tacit knowledge are not protected. In addition, unlike patents and copyrights, trade secrets laws do not protect against a rival using fair methods to replicate the knowledge concerned, and use it, nor are they binding on third parties. (Liebeskind, 1996), also stated that knowledge is difficult to protect because it’s difficult to detect its expropriation, or illegal imitation. Unlike tangible assets, knowledge is inherently mobile, because it resides in the heads of individuals, and therefore, knowledge can only be rendered immobile by deliberate actions. This sentiment was also shared by (Desouza, 2006).

Then, looking at these limitless problems facing the protection of knowledge assets, do organisations have what it takes to counter all this problems? It is now evident that knowledge assets, one way or the other, have to be protected to give you a competitive edge, but given all this knowledge protection problems, how do organisations supposed to protect their knowledge assets?

1.3 Research Objectives

The main objectives of the research are to,
Study and explore how different local organizations secure their knowledge assets.

Come up with a framework/model that local organizations can use as a guidance to secure their knowledge assets in their optimal benefits.

1.4 Research Question

The question is, if securing knowledge assets is such a difficult problem;

How do organizations model their knowledge security in order to secure their intellectual assets to their optimal benefits?

1.5 Research Delimitations

This research is only concerned with knowledge assets protection factors facing the organisation as a unit. Data collection will exclude financial sectors. This is mainly due to the fact that financial institutions have strict measures that forbid sharing of critical information to the researchers.
CHAPTER 2

2. LITERATURE REVIEW

The concepts of data, information, and knowledge are closely related and more importantly are all necessary for any Knowledge Management initiative. In order to design and implement a successful Knowledge Management idea, it is vital that not only the distinction between these concepts is clear but also their interrelation. The terms data, information and knowledge are frequently used for interchanging concepts. But this does not hide away the fact that the concepts are different and they mean different things. The main difference between them lies in the levels of abstractions being considered. Data is the lowest level of abstraction, information is next, and finally, knowledge is the highest level among all the three.

2.1 What is Data?

Computers are often called data processing machines or information processing machines. People understand and accept the fact that computers are machines designed for the input, storage, processing, and output of data and information. But can we define data without the use of information? Well some authors attempted to do so. (Stenmark, 2001), compiled a list of definitions from different authors. In his compilation, just to take a few, (Stenmark, 2001), stated that data is a set of discrete facts, or data is text that does not answer questions to a particular problem, or data is facts and messages. So there is data and information, which one makes the other? Well, in reality all these concepts are dependent on one another. Some people even use one concept to define the other.

Data on its own has no meaning. (Hole & Hawker, 2004)’s Concise Oxford English dictionary describes it as facts or statistics used for reference or analysis, and in philosophy, it is things assumed or known as facts, making the basis for reasoning. Human beings have used data as long as we existed to form their own knowledge. We tend to perceive data with our senses, and then our brain processes this data to form knowledge. Data is often said to be representing unorganized and unprocessed facts. Usually, data is static in nature. It can represent a series of discrete facts about events.
Data is a set of characters that one can read but cannot form meaning out of it. For example, if you read a barcode, one cannot make any sense out of it. All you can see is this is a series of un-identical lines with a series of numbers at the bottom and is often called a barcode. But when you put these un-identical lines under a barcode scanner you will get a vast number of information from that, such as the price of the item, the quantity, manufacture’s date etc.

2.2 What is Information?

In his report, (Floridi, 2005), stated that Claude Shannon remarked that “the word information has been given different meanings by various writers in the general field of information theory. It is like that at least a number of this will prove sufficiently in certain applications to deserve further study and permanent recognition. It is hardly to be expected that a single concept of information would be satisfactorily account for the numerous possible applications of this general field.” (Floridi, 2005) states that intuitively, information is often used to refer to non-mental, user independent, declarative (i.e. alethically quantifiable), semantic contents, embedded in physical implementations like databases, encyclopaedias, websites, television programmes and so on, which can variously be produced, collected, accessed, and processed. (Hole & Hawker, 2004)’s Concise Oxford English Dictionary, describes information as facts or knowledge learned, or just what is conveyed or represented by a particular sequence of symbols, impulses, etc.

As you are reading this material that I have gathered together for this thesis from several sources, you are actually assimilating information. What you have just read is information that you will keep in your memory, either short term or long term memory. If you forget this information, you are sure that you can always come back to get it. But that surety may not always be the case. Information stored may be lost. My thesis may be lost immediately after defence, either deliberately or accidentally. This actually means information may not always be there for you when you need it.

In the past information was something which was really hard to find. Conducting a research was extremely difficult and researchers were not coming with good results or best researches. Their researches were really limited by lack of information. So today everything is different. People even say we are now living in the world of information. Everything you need is at your disposal. There is too much information which is even threatening to
confuse us the creators of it. With the introduction of the World Wide Web, life became so easy for the researchers. They now have everything at their hands. All they need to do now is organise it in a manner that will serve their purpose. So what is really information? How does it differ with data and knowledge? Well, information is data that has meaning and one can use to solve a problem. So when you read this document, you can actually make sense out of it and you can use it to solve a certain problem. This means this document is full of information that can save somebody’s life. When you read this document it is different to reading the barcode. From this document you can make sense out of it while the barcode you couldn’t. These become the distinction between data and information. The ability to use the document to solve a problem means you have gained knowledge out of my compiled information. You can now use what you learnt from the document to solve the problem.

2.3 What is knowledge?

In the past organizations were locked in the struggle to out–do one another. But this seems to be the challenge of the past. Organizations are now struggling to out–know one another. How do these organizations out–know one another? What is the purpose of out–knowing each other in the first place? Well the answer is best known to them. But one thing for sure is of vital importance to achieve this. They should have knowledge and the knowledge to manage their knowledge. So what is this knowledge? Do I have knowledge too? The answer is definitely yes. Almost every individual has knowledge. What we don’t know is what knowledge is. (Sundgren, Marrensson, Mahring, & Nilsson, 2003), stated that human beings have always created and processed information and knowledge in their minds. They have also, long before computers were invented, produced and processed data.

The definition of Knowledge has never been exact. Different authors have different thoughts about what knowledge is. (Stenmark, 2001)’s report described knowledge as the ability to assign meaning. It is valuable information from the human mind. (Stenmark, 2001)’s report also described knowledge as text that answers the questions why or how. Lars Qvortrup, (The Public Library: From Information to Knowledge Management: a Theory of Knowledge and Knowledge Categories), describes knowledge as confirmed observations and is confirmed over time or in society.

So what is really knowledge? If I write a book for example, and give it to you to read, am I giving you my knowledge? Well, the answer might be not too precise. (Lehrer, 1990),
stated that all agree that knowledge is valuable, but agreement about knowledge tends to end there. The author states that philosophers disagree about what knowledge is, about how you get it, and even about whether there is any to be gotten. Epistemology, the theory of knowledge, and metaphysics, the theory of reality, has traditionally competed for the primary role in philosophical inquiry (Lehrer, 1990). Epistemology asks what we know, and the metaphysician what is real. Well, my concern in this thesis is epistemology not metaphysics. The thesis is more concerned about how organizations can protect what they know, not what is real, and as such the debate between epistemology and metaphysics will not take centre stage.

(Aune, 2008), stated that the principal meaning of the word knowledge can be arranged into three groups. The first group concerns abilities of various kinds, primarily cognitive abilities that result from learning but sometimes even motor abilities. For example, one can know English, or know how to walk on stilts; one can know how to give a rousing speech, how to use the library, how to get to the airport, but also how to use a handstand or back flip. Another group involves acquaintance, familiarity, personal experience, and corresponding recognizable abilities. For example, one can know a former teacher; one can know a person by name or sight; one can know fear, love or disappointment; and can know Lulea, or the neighbouring university campus. The last group concerns facts gathered by study, observation, or experience, and conclusions inferred from such facts.

Knowledge exists in two forms, tacit and explicit knowledge.

2.3.1 Tacit Knowledge

The salient characteristic of the tacit knowledge approach is the basic belief that knowledge is essentially personal in nature and is therefore difficult to extract from the heads of individuals (Sanchez, 2004). He states that, in effect, this knowledge management approach assumes, often implicitly, that the knowledge in and available to an organization will largely consist of tacit knowledge that remains in the heads of individuals in the organization. (Jasimuddin, Klein, & Connell, 2005) state that, tacit knowledge, as originally characterised by Polanyi, is constructed from individuals' own experience in the world and forms the basis for explicit knowledge. They state that tacit knowledge represent knowledge that people posses. It is embodied in the human brain and cannot be separated from the people who poses it, and it derives from the background and experience of the individuals.
who possess it and thus highly idiosyncratic. As a consequence, it is more difficult and costly to access than explicit knowledge.

2.3.2 **Explicit Knowledge**

In contrast to views held by tacit knowledge, the explicit knowledge approach holds that knowledge is something that can be explained by individuals, even though some effort and even some forms of assistance may sometimes be required to help some individuals articulate what they know. As a result, explicit knowledge approach assumes that the useful knowledge of individuals in an organization can be articulated and made explicit (Sanchez, 2004). He states that working from the premise that important forms of knowledge can be made explicit, the explicit knowledge approach also believes that formal organizational processes can be used to help individuals articulate the knowledge they have to create knowledge assets. (Jasimuddin, Klein, & Connell, 2005) state that explicit knowledge represents knowledge that can be codified in a tangible form. Thus it can be codified, documented and transmitted, making it easily and cheaply to larger numbers of people at little or no marginal costs.

(Al-Hawamdeh, 2002) argues that knowledge embodied in books and journals does not necessarily translate into useful and usable knowledge unless it is read, manipulated and communicated from one person to the other. In other words, he says, knowledge can only reside in minds of people and the minute it leaves the human mind, it is information. Does this mean explicit knowledge is information? Well, according to my interpretation of his statements, this seems so, and it also gets my full support, that knowledge stored in books and journals is information. (Al–Hawamdeh, 2002) confirms that by stating that “everyone is more or less agreed that explicit knowledge is information”. The distinction between the two terms comes in the level of abstraction. Now to answer the question; if I give you my book to go and read, am I giving you my knowledge? The answer would be, that book will only become knowledge to you only after you read it, understood it, and being able to use whatever is written in it to solve a problem. This actually means you have gained knowledge from reading my information.

2.3.3 **Knowledge Assets**

(Hole & Hawker, 2004)’s Consice Oxford English dictionary describes an asset as a useful or valuable thing. In other words, knowledge assets is knowledge that is regarded as valuable
within the organisation. Not all knowledge in an organisation has value. For example, knowing how to make best cookies is of no value to the organisation that specialises in network defense, but having knowledge about the threats facing an organisation can be of great value. Knowledge assets, according to (O'Donoghue & Croasdell, 2009) are generally non-tangible. They are rarely recorded on a balanced sheet even though they have a direct impact on the market value of the organisation. (O'Donoghue & Croasdell, 2009) state that these assets can be viewed in terms of human capital, structural capital, and innovation capital. Human capital in this case is the combination of knowledge, skill, innovativeness, and ability of individual employees. Structural capital is the knowledge embedded in the routines and processes within an organisation that contain non-human stores of knowledge. Innovation capital is an organisation’s ability to create change. This change can come in the form of innovative products, services, or internal processes. Examples of knowledge assets as provided by (O'Donoghue & Croasdell, 2009) include brand name, brand images, source code, even process knowledge, complex algorithms, and even employee competency.

(SMR International, 2008), defined knowledge asset as any collected information or knowledge held by the larger enterprise and used by anyone affiliated with the organization to help the organization achieve its goals. It is often thought as an organized content to get something done. (SMR International, 2008), continued to state that we might also think of a knowledge asset as anything within our organization we are able to refer to as we make decisions, attempt to accelerate innovation, or conduct a research.

The information, knowledge, or strategic learning content of knowledge assets, according to (SMR International, 2008), is related to but distinct from tangible assets, monetary assets, and the traditional accounting concepts applied to intangible assets. Examples of knowledge assets according to (SMR International, 2008) include any collection of knowledge of value to the organization, including documents, databases (externally leased or purchased or created internally), reports, research materials, taxonomies, glossaries of terms as applied in particular environments, and similar collections of captured information. Additionally, knowledge assets include individuals and groups of individuals, networks, project teams, communities of practice, and links to these groups and the materials and comments about experiences they create as they work together, captured in the context of that shared work experiences. Knowledge assets can also be viewed as intellectual assets or just intellectual
capital. (Desouza, 2007), stated that intellectual assets can be defined as the knowledge housed in the minds of employees, encapsulated in products and services, or embedded in the internal or external networks of the organisations, which provides organisations with competitive advantage and differentiates them from competitors.

2.4 What is Organisational Knowledge?

(Kuriakose, Seetha, Murty, Athinarayanan, & Swaminathan, 1995), define organisational knowledge as combined knowledge of all past and present employees of the organisation. The authors' state that in this sense, it may not be possible to capture the complete organisational knowledge into accessible repositories because it involves tacit knowledge and it involves past employees, and however, they view the term ‘Organisational Knowledge’ to refer to the combined knowledge of all past and present employees of the organisation which are captured into accessible repositories. (Kuriakose, Seetha, Murty, Athinarayanan, & Swaminathan, 1995), stated that in the absence of organisational knowledge, other resources cannot be utilised effectively. Thus, organisational knowledge facilitates creation of new knowledge.

When differentiating personal knowledge management from organisational knowledge management, (Sanchez, 2005), stated that in contrast to personal knowledge approach, the organisational knowledge assumes that knowledge is something that can be made explicit, i.e. can be articulated and explained by individuals who have knowledge, even though some effort and assistance may sometimes be required to help individuals articulate what they know. As a result, the organisational knowledge approach fundamentally assumes that much, if not all, of the knowledge of individuals that is useful to the organisation can be articulated and thereby made explicit and available to others. Working from this premise, says (Sanchez, 2005), the organisational knowledge approach generally advocates the creation and use of formal organisational processes to encourage and help individuals articulate the important the important knowledge they have- and thereby to create organisational knowledge assets. In my understanding, what (Sanchez, 2005), is saying is knowledge that cannot be articulated and explained to individuals even through any kind of effort or assistance cannot be viewed as organisational knowledge. However, organisational knowledge can be articulated by those who have the knowledge and is often created by formal organisational processes.
2.5 **What is Optimal Benefits?**

The term optimal according to (Hole & Hawker, 2004) is an adjective that refers to best or most favourable. Benefit on the other hand is an advantage or profit gained from something. When combining the two terms to now come up with one meaning, optimal benefits would be logically defined as best or most favourable advantage or profit gained from something. In this paper, optimal benefits would be best or most favourable advantage or profit gained from securing knowledge assets within the organisation.

2.6 **Strategic Considerations in securing Knowledge Assets**

In order to build a viable security programme for your intellectual assets, in his book: (Managing Knowledge Security; Strategies for Protecting your Company's Intellectual Assets, 2007), Desouza advocates seven considerations that should be carefully thought through, not just be dealt with through operational lenses or even tactical frames, rather, they need to be considered as strategic matters. These seven strategic considerations as outlined by the diagram below are:

![Diagram showing seven strategic considerations](image)

Figure 1. the seven strategic considerations (Desouza, 2007).
✓ **Build a security team:** the individuals who build a security team are the most important assets in the defence against intellectual assets breaches and sabotages, states (Desouza, 2007). This ideal team should have several desirable characteristics. He states that first, each individual will display the outmost integrity and allegiance to the organisation. Secondly, the security team will be comprised of individuals with a wide assortment of skills and capabilities. Having only techno-geeks on your team is not sufficient, even if 90 per cent of the threats in your organisation arise from technology centred attacks. Third, the ideal security team will be comprised by a variety of experiences. Fourth, the security team must be a cohesive unit. Finally, the security personnel should be paid well.

✓ **The Public Relations Plan:** it is very important that a security group has an adequate public relations (PR) plan, states (Desouza, 2007). The PR plan must account for the two faces of the public: the internal employees of the organisation and the external stakeholders, which include business partners, government, academia and the press, among others. This PR plan play its importance in first, designating points of contact when the external world want to contact the security group, second, place an ombudsperson so that security personnel have a place to go for bringing issues to the attention of the management, third, ensures that your unit has a process for ensuring that responses to the external world are thoughtful and complete, fourth, the concerns of internal employees need to be handled with care, thus on one hand, you want to inform your employees about the safeguards that protect them and the organisation’s intellectual assets and on the other hand you must preserve the element of surprise and the clandestine nature of security operations, and finally, the security team must work hard to maintain and preserve the trust others place in it. As such a good PR plan can be a great contributor to this goal.

✓ **Evaluate the Security Function:** some vital questions to ask yourself in this section are: how do you know that the money spent on the security programme is paying off? What is the return on investment? Are the security department overly paranoid and building defences that are over the top? These are quite difficult questions to answer for one obvious reason. security questions are normally called into question when a breach has occurred. One way of evaluating the security function is to
collect the obvious measures. This will include the numbers of attacks that were attempted and failed. Data can collected on the number of breaches that occur in firms similar to yours and then compare your organisation’s numbers to this number. Data should also be collected on security interventions. All of this data made a very powerful statement to the board of directors and showed that money being spent on security is actually paying off. External experts should be brought in to test the resilience of your security programmes. And finally, remember that evaluation is as good as it is being perceived by the evaluators, and a good security function must be able to help other functions to achieve their goals.

✓ **Monitoring the Security Function.** employees are often very sceptical on the powers vested in the security function, and a good system to monitor the security function will help alleviate employee concerns and will also act as a good check and balance. This can be done by first, having a board of overseers for the security function, second, ensuring that there are checks and balances in place, third, as part of the PR plan, make it clear to the employees that the security department reports to the board, that the security department’s actions are being monitored, and that there are processes that ensure that no security action is conducted without proper authorisation.

✓ **Building or Outsourcing the Security Function:** one non trivial decision here is whether you want to outsource the management of security operations or you want to build this capability in-house. If the firm has a history of running its own security operations, (Desouza, 2007) finds it better to continue with that, unless the current operations are failing. If the firm does not have a security function for ts intellectual assets, or if the current function is not performing up to par, outsourcing might be considered. Outsourcing security requires working with a business partner, and this requires you to have an appropriate agreement in place with your security vendor, which assumes that you have thought through the issues of coordination and control. Close attention to the alliance should be considered, ensuring that you work with the security vendor to resolve issues in the early days of the alliance. The last thing to consider will be the incentives provided to the security vendor. (Desouza, 2007) states that just as you should provide the employees with incentives to uphold
security procedures and secure intellectual assets, so should you provide security vendors with incentives. Incentives should entice the security vendor to be on its best behaviour, work with alertness, and secure the intellectual assets of the organisation.

✓ **Local or Global Security**: most organisations are global in nature and are spread across multiple locations. Now the common question is, what is the appropriate governance mechanisms for security programmes? (Desouza, 2007) states that the answer to this is it depends. Organisations that operates on a franchise model, where all locations follow a similar process and practices, a unified security approach is possible, and this is because there will be economies of scale. For organisations that produce multiple products across multiple locations, a unified set of security practices will be difficult. In this case, security programmes will vary according to product or service and also by location. Each unit should be allowed to build up its own security programme to address its unique needs. The role of the overall organisation then would be to provide a general framework within which these local programmes can be constructed.

✓ **Prioritizing Goals and Objectives**: no security budget will be adequate, nor will you find an organisation devoting ample resources to security. (Desouza, 2007) states that given that you will not be able to secure all the intellectual assets in an organisation, you must prioritise where to spend your energies. If an employee possesses knowledge and capabilities that are rare, non imitable, non substitutable, and are of value to the organisation, then the organisation needs to pay attention to him or her and ensure that there are adequate mechanisms in place to protect the person’s knowledge. The most highly valued employees need to be protected first, and then you can move to the rest.

### 2.7 Identifying Intellectual Assets

(Desouza, 2007), stated that defining what constitutes knowledge and how we measure and capture knowledge has puzzled philosophers since the dawn of time. From an organisational perspective, we need to be quite specific in determining which organisational knowledge truly represents intellectual assets (Desouza, 2007). Different knowledge assets have different values attached to them, and some don’t need to be protected as they are invaluable. Not all knowledge that an employee has can be put to
productive use. Not all knowledge resources have equal importance, and some kinds of knowledge may be more valuable than others. Therefore, an organisation cannot afford to provide security to all knowledge that exist within itself.

Any asset needs to contribute value (Desouza, 2007), and value emerges when we put an asset into use. In order to use an asset, one must have the necessary capability and intent. In this context, necessary capability come down to having the organisational processes required to take advantage of the asset. Intent is the strategic direction and focus of the organisation. (Desouza, 2007) states that once we determine that a resource does in fact contribute value, the next question to ask is, what kind of value does the resource provide? At the basic level, a knowledge resource should contribute to the operational effectiveness and efficiency of the organisation. Knowledge resources at the next level up can contribute to the tactical processes in the organisation, and tactical processes represent the nature of how work is done. At the final level, a knowledge resource can be of interest for its contribution to the strategic level. Knowledge resources across the three levels; operational, tactical, and strategic need to be cared for differently. Another question to ask, according to (Desouza, 2007), is what is the future value of the asset? Is the asset increasing in value, or is it decreasing? Unless an asset has a future value, the cost one will incur in securing it will not be justified. Once we have ascertained that a given resource contributes value to the organisation, the next question to ask is, how rare is the resource? A resource that is not rare can be easily replaced. (Desouza, 2007) states that lack of rarity is commonplace when we consider knowledge resources that contribute at the operational level. Knowledge resources at the tactical and strategic levels are more likely to exhibit the characteristics of rareness. The next question to ask according to (Desouza, 2007) is, is the knowledge resources non-imitable and non-substitutable? Non-imitatable means that the knowledge resource cannot be duplicated, and copies cannot be made. Non-substitutable means that a knowledge resource cannot be replaced by a variant knowledge resource. Knowledge resources that are non-imitatable and non-substitutable, in addition to being valuable and rare, need to be given the utmost care. These knowledge resources are the highest valued intellectual assets of the organisation. (Desouza, 2007). Most knowledge resources will meet the condition of being valuable, however, only certain knowledge resources will be able to meet the condition of rarity. At the bare minimum, for a knowledge resource to qualify as an intellectual asset, it should be of value to the organisation, says (Desouza, 2007).
Just as we can segment explicit knowledge resources, (Desouza, 2007) states that we can also segment knowledge workers and the capabilities and the expertise they possess. Not all knowledgeable workers are alike, and treating them as such will result in failed management approach. Some employees work in a highly autonomous way and are highly skilled; they often know their work in great detail. Others are highly skilled, yet their work is more dependent on an external party such as a boss or a supervisor. Other types of knowledge workers are not highly skilled yet know how to follow knowledge based procedures and perform tasks. Each type of knowledge of knowledge worker needs to be managed differently, and offers different value propositions to the organisation.

To summarise, in identifying intellectual assets, the organisation must ask itself all this questions:

1. Is the resource or capability valuable?
2. Is the resource or capability rare?
3. Is the resource or capability non-substitutable?
4. Is the resource or capability non-immitable?

(Desouza, 2007) states that if the answer is yes to all questions, the resource or capability is an intellectual asset of the highest value. If the answer to question 1 is no, the resource or capability is not an intellectual asset. If the answer to question 3 and 4 are no, the resource or capability might be an intellectual asset depending on the organisational context, or they could be assets of a lower value.
CHAPTER 3

3. THEORETICAL FRAMEWORK

3.1 Knowledge the Product, Process and People

(Desouza & Vanapalli, 2005), stated that in order for an organization to have an optimal security program in place it must address the people, the product, and the process aspects of knowledge management, and failure to protect all three will result in an incomplete program. It is upon this idea that the case development for this research has been designed in order to cover knowledge security in a complete set up.

Knowledge as a product basically deals with knowledge that is already in codified form. (Cowan, David, & Foray, 1999), defined codified knowledge as, its obvious reference, is to codes, or to standards- whether of notations or of rules, either of which may be promulgated by authority or may acquire “authority” through frequency of usage and common consent, by de facto acceptance. (Cowan, David, & Foray, 1999), continued to state that models must be developed, as must the vocabulary with which to express those models, and when models and a language have developed, documents can be written. In short, we can say that knowledge as a product is knowledge that have been turned from tacit to explicit form, or just explicit knowledge. In this theory chapter, we learn of a process called externalisation, where (Nonaka & Takeuchi, 1995) described externalisation as the process of articulating tacit knowledge into explicit concepts, and in this process, tacit knowledge becomes explicit, taking forms of metaphors, analogies, concepts, hypothesis, or models. Thus, knowledge as a product is knowledge that has passed through the process of externalisation. Knowledge as a product can also be said to mean knowledge that is kept as documents.

For this research, the product level of knowledge security deals with securing knowledge that is already in codified form. The focus here is the protection of explicit knowledge, mostly represented in information documents. (Desouza, 2006), stated that findings from the current literature of information security may well be applicable at this level of knowledge security. Similar to information objects found in information systems, knowledge products need to be tagged and their repositories need to be secured. This is
highly likely to bring another interesting question of: how do we segment knowledge products in order to see which ones to give priority over others when securing them. In order to build a viable knowledge security program (Desouza, 2006), stated that it is important for an organization to realise and appreciate what truly constitute knowledge object.

Knowledge as processes deals with knowledge that is inherent or generated in organisational innovative processes and practices. (Nonaka & Toyama, 2003), stated that instead of merely solving problems, organisations create and define problems, develop and apply knowledge to solve problems, and then further develop new knowledge through the action of problem solving. (Nonaka & Toyama, 2003), further stated that the organisation and individuals grow through such process, and the organisation is not merely an information processing machine, but an entity that creates knowledge through action and interaction. In this theory chapter, we also learn about (Nonaka, 1994)’s dynamic theory of organisational knowledge creation that posits that knowledge creation is a process of continual socialization, externalisation, combination, and internalisation. (Nonaka, 1994), also stated that it can be argued that the organisation’s interaction with its environment, together with the means by which it creates and distributes information and knowledge, are more important when it comes to building an active and dynamic understanding of the organisation. (Nonaka, 1994), gave an example that, innovation, which is a key form of organisational knowledge creation, cannot be explained sufficiently in terms of information processing or problem solving, but innovation can be better understood as a process in which the organisation creates and defines problems and then actively develops know knowledge to solve them. This section actually tells us that organisational knowledge creation is a process through innovative interactions of individuals, and as such they create and solve problems which in turn create more knowledge.

For this research, the processes level is whereby the process of knowledge generation and application need to be protected from unauthorised disclosure or snooping, loss or destruction, and unauthorised modifications. The inventive processes should be protected from unauthorised access and tampering. This might be a challenge to an organization as inventive or innovative processes need to be open enough in order to be more innovative. So the challenge here is how the organization makes its inventive process open enough to include the authorised external entities but not too often so as to allow knowledge to be exploited by unauthorised entities. At this level, knowledge communication issues should be well understood. Security for the knowledge process must be encompassing of four items.
identification, authentication, authorization, and intergrity (Desouza & Vanapalli, 2005), and an agent must identify themselves before getting access to the knowledge process.

It is quite hard to talk of knowledge and then not mention the two types of knowledge; tacit and explicit knowledge. Tacit knowledge, as is widely known, is knowledge that resides in the people’s minds. In other words, we can say, tacit knowledge within the organisation is the knowledge that resides in the minds of organisation’s employees. It is also often stated that the most valuable asset an organisation has is its people and the knowledge they have. In this paper, knowledge as people deals with the human side of knowledge security. As shown in the theory chapter, (Nonaka & Takeuchi, 1995)’s ontological perspective of knowledge creation holds that at a primary level, knowledge is created by individuals, and an organization cannot create knowledge without individuals. They state that an organizational knowledge creation, therefore, should be understood in terms of a process that “organizationally” amplifies the knowledge created by individuals and crystallizes it as part of the knowledge network of the organization (Nonaka & Takeuchi, 1995).

Then, if your employees hold valuable knowledge for the organization, do they really know that they hold such valuable knowledge? How are the employees supposed to handle themselves in order to secure that knowledge? Does the organisation have the proper mechanisms to monitor such knowledge? If so, who is responsible for managing that knowledge? Take a simple case, for example, in most of the organisations, it is well common that one or two employees know how to do certain business processes and no one else does. If those employees who knows how to perform such business processes decides to leave the organization, how is the organization supposed to recover that knowledge. Recovering that knowledge may often be too difficult to do, or even impossible. This are some of the questions that you need to ask yourself when you want to deal with the people aspect of knowledge security. (Desouza, 2006), stated that in this level, knowledge security research space can gain from the extant literature in information security.

3.2 Knowledge and the Theory of the Firm

(Liebeskind, 1996), stated that transaction–cost economics suggest that a firm may have three types of advantage relative to markets for managing, or governing knowledge transactions. First, by unifying ownership of knowledge and other assets within a firm, the
incentives of the contracting parties can be better aligned, attenuating the incentives for opportunistic behaviour. Second, a firm can substitute an employment contract for a market contract for human capital services, increasing the scope of control over knowledge workers actions and/or reducing the cost of such control by replacing legal contracting with managerial fiat. Third, a firm can alter the futurity of rewards relative to market contracts, thereby reducing employee mobility.

On the incentive alignment and knowledge protection, (Liebeskind, 1996), stated that market contracts that govern exchanges of goods and services are typically incomplete; some terms and conditions of the anticipated exchange are left un-contracted, subject to later negotiations between the parties, and this un-contracted dimensions of the exchange, which are in essence property rights are called residual rights of control. When residual rights of control accrue to separate parties, these parties may have incentives to use them in their own favour, motivating self-interest and even opportunistic behaviour, and when the ownership of the assets involved in a transaction is unified within a single firm, instead, the firm becomes the sole owner of the residual rights, allowing these rights to be administered by a single managerial hierarchy (Liebeskind, 1996).

On the employment and knowledge protection, (Liebeskind, 1996), stated that a second institutional capability that allows firms to protect knowledge is their ability to write employment contracts—be they formal, written contracts or un-written contracts. When an individual becomes an employee, she is agreeing, contractually, to obey the orders of her employer. Thus a primary feature of an employment contract is rules, and through such rules, a firm can restrict the actions of an employee in ways that would not be permitted in a market contract for human capital services. Thus, employment supports the enforcement of possession rights to knowledge. (Liebeskind, 1996), stated that a number of employee conduct rules serve to reduce the mobility of employees and thereby serve to reduce the mobility of the knowledge they possess. First, most employment contracts stipulate that a fulltime employee must work exclusively for the employer in question for the duration of her employment. Second, employment contracts frequently contain confidentiality or non-disclosure clause, whereby the employee agrees in writing not to discuss the business of a firm with outsiders, and even with other employees. Third, a firm can demand that an employee conduct her work in a particular place within its premises (and not enter other
areas of its premises) and that an employee communicate with, and report to, particular other employees (and not communicate with other specific employees). And finally, a firm can write an employment contract that contains a non-compete clause that forbids an employee from working for a competitor for a given period of time after leaving the firm. (Liebeskind, 1996), also stated that within a firm, rights to monitor are far more extensive; a firm can legally monitor its employees’ telephone conversations, e-mail communications, and mail; use visual monitoring systems; and monitor and search individuals who enter and exit its premises.

On re-ordering rewards and knowledge protection. (Liebeskind, 1996), stated that a third institutional capability that may allow a firm an advantage in protecting knowledge relates to their ability to re-order rewards over time. Because knowledge- and most particularly, legally unprotected knowledge, resides in the heads of individuals, an individual who possesses valuable knowledge always has an incentive to sell her knowledge to the highest bidder, most especially by leaving a firm and going to work for a rival. However, because a firm is a long-lived institutional form, a firm may be able to increase an employee’s cost of leaving by deferring the timing at which an individual receives payments for knowledge—so called golden handcuffs. (Liebeskind, 1996), also stated that by providing credible long term incentives, a firm also increases the incentive for an employee to invest in a formal personal relationships with other employees, thereby increasing the likelihood that an employee will become emotionally attached to other employees or to the organisation as a whole, and this attachments will also increase the employee’s cost of exit. Although these mechanisms of attachment are second-order effects that depends on expectations of long-lived employment, they may nonetheless play a critical role in inhibiting employee mobility, says (Liebeskind, 1996). Long-term employment also allows management to observe the behaviour of an employee over a long period of time and better determine their trustworthiness. Finally, (Liebeskind, 1996), stated that long-term employment increases an employee’s exposure to a firm’s acculturation mechanisms. Thus, firms can influence employees’ attitude in numerous different ways, such as advocating certain personal values or attitudes (e.g. loyalty to the firm), and providing social rewards to individuals who demonstrate certain desirable behaviours (e.g. maintaining confidentiality). Attempts to influence attitudes are more effective, the longer an individual is exposed to them, and the less that individual is exposed to countervailing influences, stated (Liebeskind, 1996).
3.3 **Securing Knowledge Assets and Processes; Lessons from Defence and Intelligence Sectors**

In one of their conference proceeding paper conducted in Hawaii, (Desouza & Vanapalli, 2005) described practices and procedures in place at defence, intelligence and security organisations that enable them to secure their knowledge resources. Due to their huge success in protecting their knowledge assets, the point of the research was to get the lessons that can be learned from Defense and Intelligency Sectors in protecting knowledge assets in private sectors. Although Desouza and Vanapalli conducted their research only in DIS organisations, in this section, the paper tries to point out some concepts they described that can also be useful in securing knowledge assets in other private organisations around Botswana.

(Desouza & Vanapalli, 2005), stated that DIS organisations are in fact obsessed with making sure that only the people who meet the highest standards in terms of ethics, training, and knowledge are retained. This is the prime reason for the gruesome **training** and **indoctrination** process associated with joining any of the armed services. All DIS organisations have very strict training and indoctrination programs, says (Desouza & Vanapalli, 2005). Regardless of screening procedure and agency, once candidates pass initial screening tests a rigorous training is commissioned. It is during this training process, candidates are taught about the mission of their organisations and their roles and responsibilities. Knowledge is passed to on to the candidates via in class instructions and also field based methods such as on-job training, simulations and physical exercises. Training regiments seek to mould the character of the citizen into one that meets the characteristics of a successful organisational member

Another key characteristic of managing the people aspect of security in DIS organisations is the concept of **security clearances**. (Desouza & Vanapalli, 2005) states that DIS organisationa members have a stutas; this can be rank status (Private, Lieutanant, Captain, General, Admiral, etc) or a security clearance status (Confidential, Secret, and Top Secret). Rank status is used to identify what information and knowledge is pertinent to one’s
function in the field. This are acquired statuses, which means, that all enlisted personnel must follow a pre-defined process that governs how their ranks will change based on time in the service, skill development, and performance. DIS organisations have very clear guidelines that articulate the roles, responsibilities, access, privileges, and accountability for each rank. While rank is earned, security clearances are given, and they are given based on job functions. More especially, the information access requirements of a job function govern the security clearances. In order to acquire a security clearance, individuals have to fill out a rather lengthy information sheet, either on computer or paper, which is then used to conduct a thorough background investigation.

In DIS organisation, almost everything is documented, stated (Desouza & Vanapalli, 2005), and in DIS organisations, unlike in other private sectors where documentation comes as an afterthought, what makes documentation an interesting finding is the importance placed on the act of documentation. Due to both regulatory pressures and also their internal needs for knowledge sharing, DIS organisations realize the saliency of documentation process. (Desouza & Vanapalli, 2005) state that all DIS organisations they researched had teams in place whose sole responsibility was to document best practices and make the available as needed. Standardization of the documentation process is salient. In keeping with the theme of a hierarchical and standardized organisation, knowledge documents are highly standardized in form, enabling quicker search, retrieval, and comprehension.

**Tagging** of knowledge documents is also a useful aspect in DIS organisations. (Desouza & Vanapalli, 2005) state that DIS organisations like most government organisations are notorious for their efforts to tagging assets. Every asset from a desk, lamp, chair, personal computer, e.t.c is tagged with an identification number. Tagging is not restricted to physical assets, information documents are also tagged for identification. Each finished document, either in the form of a report, working paper, investigative report, manual, notice, circular, memo, directives, or any other variant is marked with an identification number. This identification number can be as simple as a working paper report to more complex indexing codes. Tagging of information objects helps the organisation track the documents, their movement, and utilisation. Moreover, it helps ensure traceability and connectivity among information objects. (Desouza & Vanapalli, 2005).
When tagging helps in tracking information documents, **segmenting** helps in classification of the information documents (Desouza & Vanapalli, 2005). Similar to clearances for employees, documents are segmented by security clearances and markings. Documents are marked by notations such as confidential, classified, secret, and top secret. These notions ensure that the knowledge presented in the document is controlled in terms of who might have access to it. Only organisational members who possess the necessary security clearances can be privy to material that is of a given sensitive level.

(Desouza & Vanapalli, 2005) state that knowledge is of little use to an organisation if it is not engaged in work practices. DIS organisations are no different than their private sector peers in difficulties faced when leveraging knowledge and managing the process of knowledge generation and application. (Desouza & Vanapalli, 2005) state that the process of knowledge generation and application must be protected from unauthorised modifications. The security of knowledge process must be encompassing of four items—identification, authentication, authorisation, and integrity (Desouza & Vanapalli, 2005). An agent must identify themselves before getting access to the knowledge process. Identification mechanisms enable a user, device, or process to present its credentials to a system. In armed services, identification takes the form of seeing the badge and the stripes worn by the person you are engaging in conversation with. (Desouza & Vanapalli, 2005) states that authentication schemes are plentiful in DIS arena, ranging from the use of ID badges, biometric sensors, voice recognition, and traditional passwords. There are three ways to authenticate an agent— by something the agent knows (password), by something the agent has (ID cards), and by something the agent is (biometrics). Generally, two or more sets described above are used for access to classified information. Authentication schemes and protocols are strictly enforced in DIS organisations. Integrity is concerned with protecting the state of knowledge while it is being processed and operated on, especially from malicious and accidental acts of modifications.

Knowledge is communicated via **channels**, says (Desouza & Vanapalli, 2005), and channels can range from a telephone line, e-mail, to face to face dialogues. Regardless of channel, DIS organisations have stringent security measures in place to ensure that only authorized knowledge is communicated over an authorized channel. Classified material cannot be sent over an insecure communication channel and vice versa. Failure to ensure that appropriate
channels are used could jeopardize the security of the knowledge, ultimately affecting the value of the knowledge. To counter such cases, DIS organisations must have effective security protocols in place. (Desouza & Vanapalli, 2005) states that various defense departments have devised complex text scanning algorithms, which screen network traffic to ensure that no classified information moves via insecure and unauthorised communication channels. DIS organisations have strict guidelines on how should sensitive face–to–face conversations be conducted. Communication channels are regularly monitored to ensure that they are safe for the secure transmission of knowledge, there are private sound proof rooms for engaging in sensitive discussions, and personnel are instructed to be aware of their environment before conversing on sensitive items. In addition to securing knowledge channels, DIS organisations also pay attention to the storage and processing devices. Sensitive material is not permitted out of the premises, and strict rules govern the copying, duplication, and storage of sensitive materials.

On the role of leadership in organisations, (Desouza & Vanapalli, 2005) states that first, mandatory usage of knowledge management systems should be ordered by leadership. Knowledge management systems are not optional tools, they are critical components of work practices, decision making, and task assignments. Second, leadership must seek to integrate the different functions of the organisation. Leaders focus on ensuring direction and foresight, and this is done by clear frequent, and open communication with their staff members on a regular basis. Leaders communicate with their subordinates, who then must relay information to their subordinates, and so on until the message is passed to all. Leaders also focus on ensuring goal conformity. The organisational missions are put at the forefront and all are asked to rally behind them. Leaders hold people accountable for their actions. Just like holding an employee accountable for stealing office property, we must begin to hold people accountable for the intangibles, says (Desouza & Vanapalli, 2005). Stealing a computer is not significant instead it is the stealing of the information and knowledge that resides in the computer that might do the most harm. As such, it is important to ensure the people are held accountable in how they utilize organizational knowledge in the pursuit of tasks and assignments.
3.4 Theory of Organizational Knowledge Creation

Before you can think of how to manage anything, it is always wise to know what you going to manage so that the right management procedures are used. Offering protection to a certain structure, lets say a building, requires you to know how that building looks like, and all the possible entries to that building so that constant lookout is always focused on those entries. For this research, it also wise to know how organisational knowledge is created, and how it is transformed from one individual to the other as it changes its forms, before we can even think of how to protect it.

(Nonaka, 1994)’s dynamic theory of organizational knowledge creation holds that organizational knowledge is created through a continuous dialogue between tacit and explicit knowledge via four patterns of interactions; socialization, combination, internalization and externalization. The dynamic theory of organisational knowledge creation posits that knowledge creation is a process of continual Socialization: sharing, of individual tacit knowledge; Externalization of tacit knowledge to explicit knowledge – that is, codifying tacit knowledge into metaphors, analogies, figures or stories in order to create new concepts, and then justify them in relation to corporate imperatives; Combination in which prototypes of the new concept are developed and incorporated into the organization; and Internalization of this new knowledge through learning by doing and experimentation – thus rendering the new knowledge once again tacit. Socialization, Externalization, Combination, and Internalization, according to (Nonaka & Takeuchi, 1995), is the conversion process that brings the new knowledge of individual staff members into the organization and puts this knowledge to effective use in achieving organizational vision, strategic objectives and performance expectations.

Like any other approach to knowledge, (Nonaka & Takeuchi, 1995)’s organizational knowledge creation has its own “epistemology”, although one substantially different from the traditional Western approach (which focuses on truthfulness as the essential attribute of knowledge). They state that, the cornerstone of their epistemology is the distinction between tacit and explicit knowledge. In their book (The Knowledge Creating Company: How Japanese Companies Create the Dynamics of Innovation), (Nonaka & Takeuchi, 1995), believed that the key to knowledge creation lies in the mobilisation and conversion of tacit knowledge. And because they are concerned with organizational knowledge creation, as
opposed to individual knowledge creation, their theory also have its own distinctive “ontology” which is concerned with the levels of knowledge creating entities (individual, group, organizational, and inter-organizational).

![Diagram](image)

**Figure 2. Two Dimensions of Knowledge Creation (Nonaka & Takeuchi, 1995)**

Figure 1, adopted form (Nonaka & Takeuchi, 1995) represents the epistemological and ontological dimensions in which knowledge creation (spiral) takes place. The spiral takes place when the interaction between tacit and explicit knowledge is elevated dynamically from lower ontological levels to higher levels (Nonaka & Takeuchi, 1995). The core of the theory lies in describing how such spiral occurs. This knowledge conversion (spiral) that is created when tacit and explicit knowledge interact with each other is described in four modes: socialization, externalization, combination, and internalization.

### 3.4.1 The Two Dimensions of Knowledge Creation

The epistemological aspect adopts a definition of knowledge as “justified true belief”. (Nonaka & Takeuchi, 1995), described their epistemological aspect of organizational knowledge creation by drawing Polanyi’s distinction between tacit and explicit knowledge. According to (Nonaka & Takeuchi, 1995), Polanyi describes tacit knowledge as personal, context specific, and therefore hard to formalise and communicate. Explicit or “codified” knowledge, on the other hand, refers to knowledge that is transmittable in formal, systematic language. They state that, Polanyi contends that human beings acquire knowledge by actively creating and organizing their own experiences. Thus, knowledge that can be expressed in words and numbers represents only a tip of the iceberg of the entire body of knowledge. So, in other words, in my own perceptions, explicit knowledge...
represents only a fraction of the entire body of knowledge. (Nonaka & Takeuchi, 1995), stated that, in traditional epistemology, knowledge derives from the separation of the subject and the object of perception; human beings as the subject of perception acquire knowledge by analysing external objects. In contrast, Polanyi contends that human beings create knowledge by involving themselves with objects, that is, through self-involvement and commitment, or what Polanyi called “indwelling.” To know something is to create its image or pattern by tacitly integrating particulars. Thus indwelling breaks the traditional dichotomies between mind and body, reason and emotion, subject and object, and knower and known. Therefore, scientific objectivity is not a sole source of knowledge (Nonaka & Takeuchi, 1995). They believe that much of our knowledge is the fruit of our own purposeful endeavours in dealing with the world.

The ontological aspect is the level of social relations. At a primary level, knowledge is created by individuals. An organization cannot create knowledge without individuals. Organizational knowledge creation, therefore, should be understood in terms of a process that “organizationally” amplifies the knowledge created by individuals and crystallizes it as part of the knowledge network of the organization (Nonaka & Takeuchi, 1995).

3.4.2 Conversion/Interaction of Tacit Knowledge to Explicit Knowledge

(Nonaka & Takeuchi, 1995), view tacit and explicit knowledge as totally separate but mutually complementary entities, and they interact with and interchange into each other in the creative activities of human beings. They state that their dynamic model of knowledge creation is anchored to a critical assumption that human knowledge is created and expanded through social interaction through tacit knowledge and explicit knowledge, and they call this interaction “knowledge conversion”. The assumption that knowledge is created through social interaction between tacit and explicit knowledge allowed (Nonaka & Takeuchi, 1995) to postulate the four modes of knowledge creation (Figure 4). These include creating knowledge from tacit knowledge to tacit knowledge, which is called socialization; from tacit knowledge to explicit knowledge, which is called externalisation; from explicit knowledge to explicit knowledge, which is called combination; and from explicit knowledge to tacit knowledge, which is internalization.
3.4.3 **Socialization (Tacit to Tacit)**

The Microsoft Encarta Encyclopaedia Standard 2004 explains socialization as the process by which an individual becomes integrated into a social group by adopting its values and attitudes. (Nonaka & Takeuchi, 1995), described it as the processes of sharing experiences and thereby creating tacit knowledge such as mental models and technical skills. This draws us to a point; an individual can acquire tacit knowledge directly from others without the use of language, and this is made possible through observation, imitation, and practice.

3.4.4 **Externalisation (Tacit to Explicit)**

(Nonaka & Takeuchi, 1995), explained externalisation as the process of articulating tacit knowledge into explicit concepts, and in this process, tacit knowledge becomes explicit, taking forms of metaphors, analogies, concepts, hypothesis, or models. Cyberartsweb website states that in practice, externalization is supported by two key factors:

- First, the articulation of tacit knowledge; that is, the conversion of tacit into explicit knowledge, which involves techniques that help to express one’s ideas’ or images as words, concepts, figurative language (such as metaphors, analogies or narratives) and visuals. Dialogues, "listening and contributing to the benefit of all participants," strongly support externalization.
The second factor involves translating the tacit knowledge of people into readily understandable forms. This may require deductive/inductive reasoning or creative inference (abduction).

(Nonaka & Takeuchi, 1995), argued that, among the four modes of knowledge conversion, externalization holds the key to knowledge creation, because it creates new explicit concepts from tacit knowledge. They state that the answer to, how can we convert tacit knowledge into explicit knowledge effectively and efficiently, lies in the sequential use of metaphors, analogies, and model; much to what I also believe and agrees to.

3.4.5 Combination (Explicit to Explicit)
Combination is the processes of systemizing concepts into knowledge system (Nonaka & Takeuchi, 1995). They state that this mode of knowledge conversion involves combining different bodies of explicit knowledge, where individuals exchange and combine knowledge through such media as documents, meetings, telephone conversations or computerised communication networks. Reconfiguration of existing information through sorting, adding, combining, and categorizing of explicit knowledge. Nonaka and Takeuchi believe that knowledge creation carried out in formal education and training at schools usually takes this form. In the business context, the combination mode of knowledge conversion is most often seen when middle managers break down and operationalise corporate visions, business concepts, or product concepts (Nonaka & Takeuchi, 1995).

3.4.6 Internalization (Explicit to Tacit)
(Nonaka & Takeuchi, 1995), described internalization as a process of embodying explicit knowledge into tacit knowledge, and it is closely related to learning by doing. They state that, when experiences through socialization, externalization, and combination are internalized into individuals’ tacit knowledge bases in the form of shared mental models or technical know-how, they become valuable assets. For organizational knowledge creation to take place, however, the tacit knowledge accumulated at individual level needs to be socialized with other organizational members, thereby stating a new spiral of knowledge creation (Nonaka & Takeuchi, 1995). For explicit knowledge to become tacit, it helps if the knowledge is verbalized or diagrammed into documents, manuals, or oral stories. Documentation help individuals internalize what they experienced, and thus enriching
their tacit knowledge. In addition, documents or manuals facilitate the transfer of explicit knowledge to other people, thereby helping them experience the experiences of others indirectly, says (Nonaka & Takeuchi, 1995).

3.5 Security Awareness and Training

Security Awareness and Training is paramount in ensuring that people understand their responsibilities when protecting their assets. In knowledge security particularly, where the idea is to protect the knowledge that is possessed by the organisations individuals, being aware of what to do and what not to do is crucial in making sure that this knowledge stays safe. (Wilson & Hash, 2003), stated that Federal Agencies and Organisations cannot protect the confidentiality, integrity, and availability of information in today’s highly networked systems environment without ensuring that all people involved in using and managing IT;

- understands their roles and responsibilities related to the organisational mission,
- understand the organisation’s IT security policy, procedures and practices,
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

The “people factor”- not technology, is the key to providing an adequate and appropriate level of security, and if people are key, and also a weak link, more and better attention must be paid to this asset. As such, a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organisational policies, and how to properly use and protect the IT resources entrusted to them, stated (Wilson & Hash, 2003).

(Garrett, 2004), also stated that organisations appear to understand that the vast majority of security breaches are the result of human error and the development of security policies and of security awareness training is seen as key to addressing the problems. (Garrett, 2004), found that the challenge to many organisations is to create a security-aware culture. Making staff aware of the risks and their responsibilities helps them act in a sensible and secure manner. To shift the cultural paradigms of organisations into a mode where security becomes inherent requires changes in the structure of the cultural web, and (Garrett, 2004), stated that however, a critical additional factor in achieving real cultural change is in changing the behaviours of individuals throughout the organisation to support new policies, procedures and structures. The routines ways that members of the organisation behave towards each other, and that link different parts of the organisations, compromise the way we do things around here, which at best lubricate the working of the organisation
and may provide a distinctive and beneficial organisational competency. However, they can also represent a take for grantedness about how things should happen which is extremely difficult to change. (Garrett, 2004), noted that even when the security related structures are changed, policies are developed and training given, the behaviours of managers on a day to day basis reflect a current failure in integrating security into the cultural fabric of the organisation. If the policies and practices are to be successful in preventing security breaches, they need to be adopted and practiced by every member of the organisation on a daily basis, and this is a significant cultural change on our organisational thinking and requires individuals at all levels in the organisation to take the responsibility for making a decision that either safeguards or exposes the organisation to a potential harm.

*What is Security Awareness?* (Wilson & Hash, 2003), stated that awareness efforts are designed to change the behaviour or reinforce good security practices. NIST Special Publication 800–16 then defines awareness as:

“*Awareness is not training. The purpose of awareness presentation is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT Security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audience with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.*”

There are a number of potential reasons as outlined by (Garrett, 2004), that indicates why vast majority of security breaches originate from human actions:

- People are poorly trained and have poor security awareness
- People are not motivated to perform at the required level
- People are malicious and deliberately expose the organisation to risk
- People are aware of the problem of security but as managers and employees make poor decisions.

Since there is so much literature about security awareness training and how to develop policies and training programs, this vast literature can be used to address the first three reasons that individuals may be responsible for security breaches. One example of this literature is NIST Special Publication 800–50, which also states that security awareness and training should be focused on the organisation’s entire user population, and management should set the example for proper IT security behaviour within an organisation. The publication states that an awareness program should begin with an effort that can be
deployed and implemented in various ways and is aimed at all levels of the organisation including senior and executive management. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program, (Wilson & Hash, 2003).

(Wilson & Hash, 2003), stated that an awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise. An effective IT security awareness and training program explains proper rules of behaviour for the use of agency IT systems and information, stated (Wilson & Hash, 2003). The program communicates IT security policies and procedures that need to be followed, and this must precede and lay the basis for any sanctions imposed due to noncompliance. Users should be well informed of the expectations, and accountability must be derived from a fully informed, well trained, and aware workforce.

3.5.1 The Continuum

(Wilson & Hash, 2003), stated that learning is a continuum; it starts with awareness, builds to training, and evolves into education. In this continuum, a bridge or transitional stage between awareness and training consists of what NIST Special Publication 800–16 calls Security Basics and Literacy. This security basics and literacy material is a core set of terms, topics, and concepts. (Wilson & Hash, 2003), stated that once an organisation has established a program that increases the general level of security awareness and vigilance, the basics and literacy material allow for the development or evolution of a more robust awareness program, and it can also provide the foundation for a training program.

The training level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialities other than IT security (e.g. management, systems design and development, acquisition, auditing). The most significance difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or a set of issues. The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material (Wilson & Hash, 2003). The education level will integrate all of security skills and competencies of the various functional specialities into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technology and social) and
strives to produce IT security specialist and professionals capable of vision and pro-active response.

3.5.2 **Who does what?**

(Tipton & Krause, 2003), stated that the security director has the responsibility of promoting education and awareness as well as staying abreast of the new developments, threats, and countermeasures, while association with organisations such as SANS, ISSA and CSI can be beneficial. There are many other groups and forums out there, and the director must ensure that the most valued resources are used to provide alerts, trends, and product evaluation, says (Tipton & Krause, 2003). The security department must work together with the education and training departments of the organisation to be able to target training programs in the most effective possible manner. Training needs to be relevant to the job functions and risks of the attendees. If the training can be imparted in such a way that the attendees are learning the concepts and principles without even realising how much they have learned, then it is probably ideal, states (Tipton & Krause, 2003). Training is not a “do not do this” activity- ideally, training does not need to only define rules and regulations; rather, training is an activity designed to instil a concept of best practice and understanding to others. Once people realise the reasons behind a guideline or policy, they will be more inclined to better standards of behaviour than they would if only pressured into a firm set of rules.

(Tipton & Krause, 2003), stated that training should be creative, varied, related to real life, and frequent. Incorporating security training into a ten–minute segment of existing management and staff meetings, and including it as a portion of the new employee orientation process, is often more effective than a day–long seminar once a year. (Tipton & Krause, 2003), stated that using examples can be especially effective, and the effectiveness of the training is increased when an actual incident known to the staff can be used as an example of the risks, actions, retribution, and reasoning associated with an action undertaken by the security department. When there has been an incident or employee misuse, bringing this into the open (in a tactful manner) can be a way to prevent others from making the same mistakes. The attitude of the trainers should be to raise the awareness and behaviour of the attendees to a higher level, not to explain the rules as if to criminals that they had “better behave or else”, stated (Tipton & Krause, 2003).
3.6 **The Incentive Theory of Motivation**

One of my arguments in the problem description is that, many organizations don’t see that, the most secure and impenetrable defences are useless if they cover only a portion of what need to be protected, as they don’t realise that protecting cooperate knowledge has more to do with people than it does guards and technology. (Desouza, 2007) stated that, knowledge resides in the minds of employees, is embedded in work processes, and is captured in product and service offerings. A question one may ask is, can these employees be motivated to secure intellectual assets, or at least act in ways that can secure organizational knowledge? In other words, can motivation to the employees in an organization help in securing knowledge? If so, how and what kind of motivation do they need? When addressing the importance of security awareness and training, (Garrett, 2004), stated that a critical additional factor in achieving real cultural change where security culture becomes inherent is in changing the behaviours of individuals throughout the organisation to support new policies, procedures and structures. However, what (Garrett, 2004), does not discuss is how such individuals behaviour is changed. This is one area where incentive theory of motivation comes into use.

While other theories of motivation support the belief that the cause of response is internal, the incentive theory of motivation says that in fact environment brings out behaviour. The basic concept behind the incentive theory is goals. When a goal is present, a person attempts to reach that goal. (Hargie, 1997) states that incentive theory was postulated, underlining the importance the importance of external incentives as a motivation for behavior. Incentive is activated through anticipation for a desired goal, says (Hargie, 1997). A central tenet of this theory is that we seek positive incentives and avoid negative ones. Thus, when hungry, food will be a positive incentive and approached. On the other hand, the sight of a boring individual would be a negative incentive and so avoided.

Incentive theory is primarily a psychological term, explaining the relationship between motivation and behaviour of an individual, as shaped by a profitable intent. The incentives shape the behaviour of individuals. These incentives need not necessarily be monetary. They can be non–material forms like love and respect among others. Incentive theory posits that a person’s actions always has social ramifications, and if actions are positively received people are more likely to act in this manner, or if negatively received people are less likely to act in
this manner. Incentive theory of motivation holds that there is no free will as commonly conceived, but only responses to perceived pleasures and pains.

Generally, the incentive theory of motivation rests on the assumption that any behaviour that is positively reinforced (i.e. rewarded) will repeat itself, especially over time, secondly, this repetition over time, will lead to desired behaviour becoming a habit (Johnson, 2010). The theory posits that an organism is a complex object that is a product of its environment. What this actually means is that object behaviour over time can be predicted on the basis of its previous experiences. Things that have provided its pleasure will be pursued; things that provided it pain will be ignored.
CHAPTER 4

4. METHODOLOGY

The aim of this chapter is to give a highlight about the general research methodology used in this study, as well as the specific tools used in data collection and analysis.

4.1 Research Purpose

Exploratory research, also termed as formulative study, has its main purpose as that of formulating a problem for more precise investigation or of developing the working hypothesis from an operational point of view, (Kothari, 2004). The major emphasis of such studies is on the discovery of ideas and insights. (Schwab, 2005) states that empirical procedures and outcome inevitably play a more influential role when the research is not motivated by theory and such researches are exploratory. Exploratory research studies are aimed at discovering interesting relationships that may obtain in a set of data. This research is warranted when an interesting issue has not been subject to prior theory or empirical research. Exploratory research is primarily used to get deeper understanding of something. For example, knowing that there exists a computer called mainframe does not necessarily mean you know how that computer works. To get a deeper insight of how mainframes work an exploratory research would be the right research purpose to use. Exploratory research differs with descriptive research in the sense that unlike exploratory research, descriptive research cannot describe what caused a situation. Thus, descriptive research cannot be used to create a causal relationship, where one variable affects another.

The purpose of this research is to explore how organisations around Botswana make sure that their knowledge assets are protected. The idea is to get a deeper insight of how they secure their knowledge assets, and then finally propose a framework they can use to successfully protect their knowledge assets. In short, the purpose of this research is exploratory in nature.

4.2 Research Approach

Qualitative research, according to (Dawson, 2002), involves studies that do not attempt to quantify their results through statistical summary or analysis. Qualitative studies typically involve interviews and observations without formal measurement. A case study, which is an
in-depth examination of one person, is a form of qualitative research. (Dawson, 2002) states that qualitative research explores experiences through such methods as interviews or focus groups. It attempts to get an in-depth opinion from participants. (Creswell, 2007) states that qualitative research begins with assumptions, a worldview, the possible use of theoretical lens, and the study of research problems enquiring into the meaning individuals or groups ascribe to a social or human problem.

(Creswell, 2007), stated that qualitative research is used when a problem or issue needs to be explored. This exploration is needed, in turn, because of the need to study a group or population, identify variables that can be measured, or hear silenced voices. According to (Creswell, 2007), qualitative research is conducted because we need a complex, detailed understanding of the issue. This detail can only be established by talking directly with people, going to their homes or places of work, and allowing them to tell stories unencumbered by what we expect to find or what we have read in the literature.

I then believe my research is of a qualitative approach. The research need not to know any statistical analysis as the quantitative approach suggest. In fact, the need to conduct this research is to know the complex and detailed understanding of how different organizations around Botswana do model knowledge security in order to secure their intellectual assets.

4.3 Research Strategy

Case study research involves the study of an issue explored through one or more cases through a bounded system (Creswell, 2007). It is a qualitative approach in which the investigator explores a bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of information (e.g. observations, interviews, audio visual materials, and documents and reports), and reports a case description and case based themes (Creswell, 2007).

(Creswell, 2007), also stated that qualitative case studies are distinguished by the size of the bounded case, such as whether the case involves one individual, several individuals, a group, an entire program, or an activity. They may also be distinguished in terms of the intent of the case analysis, and three variations exist in terms of intent; the single instrumental case study, the collective or multiple case studies, and the intrinsic case study. In a single instrumental case study, the researcher focuses on an issue or concern, and then
selects one bounded case to illustrate the issue. In a collective case study (or multiple case studies) the one issue or concern is again selected, but the inquirer selects multiple case studies to illustrate the issue. The intrinsic case study focuses on the case itself (e.g., evaluating a program, or studying a student having difficulty) because the case presents an unusual and unique situation.

(Gerring, 2007) stated that a case connotes a spatially delimited phenomenon (a unit) observed at a single point in time over some period of time. It comprises the type of phenomenon that an inference attempts to explain. A case study will then be understood as an intensive study of the single case where the purpose of that study is—at least in part—to shed light on a larger class of cases (population), says (Gerring, 2007). An additional implication of the term ‘case study’, according to (Gerring, 2007), is that the unit(s) under special focus is not perfectly representative of the population, or it is at least questionable.

This research therefore, has been designed in form of a case study, a single instrumental case study to be more precise. The case in this situation would be designed/formed from the five organisations that will be selected to form the sample frame of organisations around Botswana. The research focuses on an issue or phenomenon, which is “how do organisation protect their knowledge assets” and it is explored in three different levels; the product, the people, and the process. In other words, the case (5 selected organisations) under focus (how can they better protect their knowledge assets?) will at least shed light on how the entire organisation in Botswana can better protect their knowledge assets.

4.4 Data Collection Method

(Creswell, 2007) describes the data collection in a case study research as typically extensive, drawing on multiple sources of information, such as observations, interviews, documents, and audio visual materials. He states that case study research is a qualitative approach in which the investigator explores a bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of information (e.g., observations, interviews, audio visual materials, and documents and reports), and reports a case description and case based themes.

For this research, interviews, observations, documents and reports have been used as a form of data collection. Both closed and open ended questions were used during the interviews.
and the interviews were performed in two styles; respondents were provided with questionnaires to feel it, while others were interviewed on face to face. Books and reports such as (Desouza, 2007), and (Desouza & Vanapalli, 2005) were very useful during the data collection.

### 4.5 Analysis Plan

Data analysis would be refined throughout the entire research process. During data collection, when new information that was not anticipated in the research emerges and appears to be relevant to the research, the interviews and interview schedules would be refined to anticipate such information, and the new information would be included in the theory chapter also. Particularly, coding, pattern coding, and data visualisation in a matrix were techniques used to analyse the data (Miles & Huberman, 1994). Coding is the process of labelling the researcher's interpretations of units of meanings in the data. This is where segments of data are summarised. Pattern coding then, is a way of grouping those summaries into emerging themes that are explanatory or inferential in nature.

With regard to the theoretical framework of the study, data analysis is done in relation to knowledge security as a product, process, and the people. Pattern coding will then be used to examine the coded data to find categories for each respondent. For each studied organisation, categories for each respondent would be compared to other respondents’ to uncover categories shared across all group members. Data from each respondent within the studied organisations will then be re-examined, to validate whether the newly emerged categories would represent each respondent coded data and my interpretations that had emerged during the course of the interviews. Finally, validated categories from all the studied organisations would be compared for some abstract analytical categories that would be shared across the organisations. Since a single case study, broken down into three sub cases has been developed, I have reduced and displayed only the important data for the research.
CHAPTER 5

5. EMPIRICAL SETTINGS AND DATA

This chapter represents the empirical settings where data have been collected and the summary of data collected by responses from the interviews. Data was gathered for this research from a wide range of sources. The collected data was all qualitative in nature. Five local organizations have been selected for data collection. Both subjective and objective data have been gathered and evaluated against security practices and literature. The data collection was designed in three levels; the product, the people, and the processes.

The selection for units of analysis was based on the fact that such units should at least resemble all organisations in Botswana. Thus, units from different backgrounds such as from government sectors, private sectors, non-governmental organisations, parastatals etc., were used as a sample frame for all organisations in Botswana. This although, excludes financial sectors, but this does not necessarily mean they are not affected by the findings of the research. In the below units, there is a government sector, a private sector, and three parastatals. This was mainly to avoid selecting units of analysis in one domain and then end up falsifying the generalisation of the research findings. Then the selected units of analysis should have at least a well-documented IT structure with a well-defined management. The point is, the case design is sectored into three levels, the product, the people, and the process level, and in order for such levels to be all achieved, and a well-documented IT structure should be in place. Lastly, the units of analysis were based on who was willing to give the information needed by the research.

5.1 University of Botswana (UB)

I have interviewed one IT technician within the Computer Science department, one Database Administrator and the Network Manager within the University IT department.

General Background

University of Botswana is the largest and highest learning institute in Botswana which aspires to be the leading centre in academic excellence in Africa and the world. The University of Botswana is a government owned entity which is run as a parastatal
organization, and it gets most of its funds from the government. It consists of eight (8) faculties, mainly; Business with three (3) departments, Education with ten (10) departments, Engineering and Technology with six (6) departments, Humanities with seven (7) departments, Health Sciences with two (2) departments, Social sciences with nine (9) departments, Science with seven (7) departments, and Graduate studies as a department on its own. The IT department overlooks the enter network of the university, and it has divide itself with different subnets for each faculty. In each department, there are at least two IT technicians and one senior technician who manage each subnet. Apart from providing IT resources to each faculty, the IT department also provides IT resources to the administration department, and other non-academic staff. The IT administration is housed in one building while faculty technicians have their offices in their respective faculties.

The role of IT Technicians is to install, modify and repair computing equipment and software, providing hardware, software and network access to the users, and also provide technical training to the users. The role of the Database Administrator is to analyse and monitor database performance and assist in resolving database problems, developing small applications and interfaces, to the university business database, and developing ad-hoc reports to user requirements. The role of the network manager is to plan, design, and coordinate implementation and management of computer networks within the university and associated external services.

Data Summary

When asked on how they secure knowledge that is already codified and kept as documents, the respondents wanted to know how does that codified knowledge differ from information. They stated that currently, they don’t have anything specified as knowledge security, and if ever they will have, maybe it will be in the future. At the moment they have only information security.

“As far as I’m concerned, knowledge is what is in someone’s head. How do you secure something in someone’s head”, (asked the networks manager)?

However, the respondents acknowledge that they do have vital information that is kept as documents in their networks e.g. students marks, personal information about employees, to say the least, that is safely stored in their networks. They state that any information that is
deemed sensitive to the public is clearly marked and stored in highly secured places. Information that is not in the hands of the IT department is upon the departments in question to make sure that such information is kept safe. As the IT department, they provide periodical trainings and awareness to all the employees of the organisation on how to handle their information and make sure that it is safe.

“We use markings such as top secret, confidential, and for official use only, to classify our information documents. We have authentication mechanisms throughout the university to make sure un-authorised people are denied access. We also use layered-defences to secure our networks, e.g. we have different types of firewalls, intrusion detection systems, physical security staff, and some of our servers are placed in the demilitarized zone”.

The respondents however, stated that they do codify some of the knowledge within the organisation, but not so often. Codification is done only when such knowledge is deemed very important while the source is from outside the organisation.

“Oh yes, we sometimes jot down some notes when we have someone from outside talking about something we don’t know, and it usually happens when an external consultant has been hired to do a certain job for us”.

On how they protect their knowledge assets from the people side, the respondents stated that they rely heavily on their training and awareness programs. They stated that even without training and awareness programs, people by default know what is sensitive and what is not, and as such they can protect the university’s knowledge by default. The stated that the fact that the university is generally one of the most respected organisations, its employees try by all means to protect its name so they can also be respected. They also they have security policies in place to show people the way in protecting their assets. These security policies are placed in the university intranet (tirisano) and anyone who has access to it can see them. Respondents stated that they never codify knowledge to cater for departing staff. They stated that their staffs are working as team and as such knowledge that is carried by one employee is also in other team members.

On the security of processes of knowledge generation and application, the respondents stated that once again, training and awareness programs are vital in educating employees
about the protection of knowledge generation. The respondents however, stated that they don't have training and awareness programs that specifically target protection of knowledge generation processes but rather they focus on information security. Whatever employees are not supposed to share with un-authorised people is classified as sensitive information not as knowledge generation process.

Respondents stated that they are not in a position to identify knowledge assets in the university networks. They stated that for them to identify all knowledge assets, first they will have to be educated on what entails knowledge assets and what not. They stated however, that they are not in possession to identify compromised knowledge assets since they can’t differentiate knowledge assets with information assets.

Although the respondents

5.2 Ministry of Health (MoH)

I have interviewed the IT manager, two systems analysts, and two users of which one is from the ministry management department and one from the health sector relations & partnership department.

General Background

Ministry of Health (MoH) is a government ministry which has the portfolio responsibility to provide leadership on health matters around the country, and it does this by formulating policies ensuring their correct interpretation and implementation throughout the health care delivery system. MoH’s data network is linked to the entire government general data network (GDN) and all its staff are seconded from Ministry of Communication Science and Technology (MCST) which manages the entire government data network. This means MoH has an IT department whose staff is the employees of another ministry (MCST). MoH has more than 16 servers and 6 of them are located within the ministry while the remaining ten servers are located at MCST.

The IT manager is responsible for the general management of the IT department including planning for IT policies and infrastructure. The systems analyst is responsible for the day to day activities of the IT department including giving access to the users and maintaining IT
systems and hardware. The users are the people who use IT systems to do their day-to-day activities in their respective departments.

Data Summary

When responding on how to protect documented knowledge, the respondents stated that information security is what they have not knowledge security.

"What is knowledge security anyway?"

Although their information security is managed from DIT, the respondents stated that they have never seen anything classified as knowledge security. They stated that whatever is kept as a document is deemed information and they use traditional information security technology such as firewalls to protect their information.

"The last time I dealt with that word is during my university times when I was doing knowledge management course, and not here. Everything here is about information and information security".

Information that is saved as documents is often kept in secure places such as locked cabinets, and the responsibility of granting access to such information lies with the respective departments. Supervisors of such departments are responsible for making sure that only authorized people have access to that information. They stated that their information documents are often classified as confidential and for official use only. The respondents stated that generally, they never codify any knowledge within the ministry.

"I won’t say we have a way of codifying knowledge within the organisation. Why would we do that anyway since we have documents that describe every detail about our systems saved in our intranets?"

The users stated that they know nothing about knowledge security and it was their first time to hear about it. They were quick though to assert that they have never attended any information security training despite their considerable time since they joined the ministry. They stated they have never been approached regarding any information security training by the department in charge. However, the IT department stated that although DIT is responsible for handling security trainings, they know that such trainings sometimes are
conducted even though sometimes it takes time for them to be done. They stated that they are not in a position to tell who attended trainings and who is not because sometimes they are not even made aware of any trainings taking place.

The respondents stated that they don’t have any particular mechanism they use to make sure that people protect knowledge assets and the knowledge they have about the organisation. Security policies are usually the only tool they use to make sure that people know what to protect assets within the ministry. These policies are never signed by employees when signing employment contracts but they are kept in the ministry intranet and assumed all will see them. The respondents stated that they can’t identify knowledge assets within the organisation because they have never classified anything as knowledge assets before.

5.3 HiPerformance Systems Botswana (HPS)
I have interviewed the Lead Enterprise Consultant, one Systems administrator and two Systems Analysts.

General Background

HiPerformance Systems Botswana (HPS) is a leading technology solution provider in Botswana that has provided a range of technology implementation services to organizations of all sizes since 1994. HPS is also a Microsoft Gold Certified Partner and an HP Partner. HPS has about fifty (50) employees, fifty-five (55) desktops, eight (8) servers, and a variety of management, backup, and security software. HPS operates by providing IT administration and consultancy to other companies, while also selling hardware and software products to these organizations.

The Lead Enterprise Consultant is responsible to plan, design, and coordinate the working relations with the external organisations which HPS offer consultancy work to. He/she also manages and coordinates the acquisition of new infrastructure as per the organisational needs. The role of the systems administrator is to offer networks and systems administration to the organisations getting services from HPS. The role of the Systems Analysts is to maintain computer systems including reviewing, analysing and modifying computer programmes, testing and installing computer systems, developing new computer systems for the organisation.
Data Summary

The respondent stated that although they recognise what knowledge is and how the protection of knowledge assets can be beneficial to their organisation, they don’t have anything specified as knowledge security. They stated that not even the organisations they provide consultancy to have anything to do with knowledge security. The Lead Enterprise Consultant stated that though they don’t have anything as knowledge security in their policies, he can see that indirectly they do have and they have a way of protecting their knowledge assets. The only problem he sees is that knowledge security is not well defined concept in their organisation due to lack of awareness from the top management. He stated that he had long wanted to sell the idea of having well defined policies of knowledge security to the management of the organisation but he just didn’t have enough information on how to go about it.

“Well, listening to how you explain knowledge security makes me realise that we do have it here, it’s only that we are not aware that we have it and it’s not well defined and integrated in our policies. I have long wanted to propose that but I just didn’t know how to start because I didn’t have enough to convince people here.”

Realising that indeed information that is kept as documents, one way or the other, is also knowledge often referred to as codified knowledge, the respondents acknowledge that they do have codified knowledge and they use traditional security technology to secure their codified knowledge.

“My friend, we have powerful firewalls and intrusion detection systems here that are supported by dedicated staff. On top of that, we have also powerful anti-viruses that are updated regularly. Don’t forget that we are a gold Microsoft partner, they give us all the necessary support when we need it.”

The respondents acknowledged that they do a lot of knowledge codification in their organisation. They stated that since they are responsible for handling systems and data from different organisations, they are forced to know and be sure with what they are doing, and as such they do take a lot of notes whenever they are taught about something new or whenever they are in an unfamiliar environment. However, they noted that their knowledge codification only happens when they take such notes and they are often
documented formally and kept safe for next use. They acknowledged that they sensitive data are often tagged as either confidential, highly confidential, and for official use. Information that is meant for public consumption is often never tagged. The respondents also acknowledge that they do segment their documents for easy identification.

On how they protect their knowledge assets from the people side, the respondents also stated that they do rely heavily on their training and awareness programs. They stated that their staffs are professional enough to be able to see what can cause harm to the organisation. They stated that the security policies in place are able to show their staff what to do and what not do, and the consequences of any breach of conduct. However, none of the employees have ever signed any policy or availed to them at a time when employment contracts were signed. Such policies are said to be placed in the department network, but some of the employees acknowledged that they have never seen such policies even though they know that they do exist. However, staffs are constantly reminded about the acceptable practices and procedures by the top management, and the importance of such practices to the organisation.

When quizzed on how they make sure that when staff leaves the organisation the knowledge they carry is retained within the organisation, the respondents stated that they don’t have any mechanisms to deal with that except persuading the staff with better incentives to abandon their motives. If such persuasion is not enough, there is nothing they can do than to let those people, and they stated that they is nothing they can do retain the knowledge of those people. They also stated that the security of the processes of knowledge generation and application relies on the security training and awareness programs, the security policies, and the security technology the employed in the organisation.

5.4 Department of Water Affairs (DWA)

I have interviewed one senior systems analyst, who was acting as the IT manager by the time, one IT technician, and one user from the water engineering department.

General Background

The Department of Water Affairs (DWA) is a government parastatal organization and is one of the three technical departments within the ministry of Minerals Energy and Water Resources. Department of Water Affairs has the national responsibility for policy, planning,
assessment, development, supply and protection of Botswana’s scarce water resources. Its head offices are located in the southern side of the city centre (Gaborone) and it has several other departments within the city and country wide. The IT main office is located in the head office with more than 15 IT officers country wide. Unlike other governments departments, DWA hires its own IT staff, and all the IT services are managed from the main office in the head office.

The role of the Senior Systems Analyst at the time of the interview was to plan, organise and manage all the IT systems, networks and the staff. He was viewed as the middle man between the IT staff and the organisation management and responsible for proposing all the IT policies to the management. The role of IT Technicians is to install, modify and repair computing equipment and software, providing hardware, software and network access to the users, and also provide technical training to the users. The User was the person who was using IT systems and equipment from the water and engineering department.

Data Summary

Responding on how they secure their codified knowledge, the respondents stated that they don’t have anything defined as knowledge security within their policies. They stated that as far as they are concerned, information security is what they understand and have in their organisation. After explaining to them how codified knowledge is the same as information, they then acknowledged that if that’s how it is, then it was not in their attention. They then stated that the use traditional security technology to secure the information residing in their networks. They stated that, specifically, they use proxy servers, packet filtering firewall, an intrusion detection system, and different types of anti-viruses (notably Symantec endpoint and Kaspersky).

“What’s the difference between codified knowledge and information? If codified knowledge is the same as information, then why do you want to refer to it as knowledge rather than information? But it sounds interesting though”.

Although some of their documents are classified, most of such documents have not been tagged, and they stated that the reason for that is because they are often kept in locked cabinets. They stated that such cabinets are always locked and only few authorised people have access to them. One respondent even stated that he once came across a document
which was not tagged but the information looked too confidential for his consumption. He stated that the incident happened when he was sent by his boss to go and look for some files in the same cabinet where he found the document. The respondents acknowledged that although they try their best to improve the situation, they can still see that their security is not the best, and often some sensitive information can be seen misplaced everywhere.

The respondents stated that knowledge codification is rarely done if ever it is. They stated that they have no plans at the moment of codifying knowledge that is carried on the employees’ heads. However, they stated that if ever is possible to document knowledge carried in people’s heads, it would be a very important thing to the organisation, but they just don’t see how that is possible.

“To be honest with you sir, this thing of knowledge security is very difficult thing which not everyone can be able to understand. I just don’t see that happening here soon, I’m not even sure I understand it myself.”

The respondents stated that the organisation relies on the security policies to make sure that employees handle themselves in the acceptable manner. However, employees are never made to sign these policies nor availed to them during signing of employment contracts. The respondents also stated that their trainings and awareness programs help them in making people aware of the security of their information. But when quizzed on when is the last time these trainings took place, the respondents could not remember that and they just said it’s been while. They couldn’t also state clearly on such training are applied in the organisation. Quizzing the users if they have ever attended any information security from their IT department, none of them answered in positive, and they divulged that the only training they can remember of is only when they are taught how to use new systems or new hardware. On whether they have seen any pamphlets that could have been meant to educate them about how to protect their assets, the users stated that they only hear about information security when they are edged not use memory sticks from other computers as they will infect their computers with viruses.

On the security of processes of knowledge generation and application, the respondents stated that they rely only on the security technology they have such as firewalls and intrusion detection systems. Otherwise they can only hope that their security policies can
help them protect their assets. Respondents were also not in a position to identify knowledge assets in their organisation. They stated they don’t know what entails knowledge assets and what does not entail knowledge asset, and as such they are not in a position to say this are our knowledge assets.

5.5 Air Botswana (AB)

I have interviewed the IT manager, two senior support officers, and the commercial manager.

General Background

Air Botswana is another government parastatal organization, and it is the only local airline that offers air routes around and outside the country. Air Botswana falls under the portfolio of Ministry of Works, Transport and Communications and it receives its funds from the government. Their WAN consists of mainly six LANs; the main LAN in Gaborone where their head offices are, and the other LANs are in Johannesburg, Harare, Francistown, Kasane, Maun, where they have sales offices. The management of their WAN takes place in the head office, and all their IT staff is located in the head offices. IT personnel move to other LANs only during time of support, and sometimes they conduct their support through the phone with the sales offices located in those LANs. Air Botswana has about six (6) IT officers and all of them joined the airline in the last three years from different companies.

The role of the IT manager was to oversee, organise and control all the IT operations including management of all the IT staff. The Senior Support officer’s role is to provide all the user support services including granting systems and networks access, network performance monitoring, software and hardware access, and hardware maintenance. The role of the commercial manager is to overlook the sales of the organisation services to the general public.

Data Summary

When asked on how they secure knowledge that is already codified and kept as documents, the respondents stated that they haven’t heard of such thing in their work place.
“Man what is that? Is it something we can do here?”

However, the respondents also acknowledge that they do have vital information that is kept as documents in their networks. They state that although most of their documents are not tagged, any information that is deemed sensitive to the public is stored in highly secured places such as locked cabinets. Information that is not in the hands of the IT department is upon the departments in question to make sure that such information is kept safe. As the IT department, they provide periodical trainings and awareness to all the employees of the organisation on how to handle their information and make sure that it is safe.

The respondents however, stated that they do codify some of the knowledge within the organisation, but not so often.

“*We sometimes write down some notes when we hear something we are not familiar with.*

On how they protect their knowledge assets from the people side, the respondents stated that they also rely heavily on their training and awareness programs. They also they have security policies in place to show people the right procedures in protecting their assets. These security policies are however, never signed by the employees. Respondents stated that they have no means of extracting tacit knowledge into explicit forms. They stated that they are not sure if such is part of their job, and if so, they were never made aware of that.

On the security of processes of knowledge generation and application, the respondents stated that once again, training and awareness programs are vital in educating employees about the protection of knowledge generation. The respondents also, stated that they don’t have training and awareness programs that specifically target protection of knowledge generation processes but rather they focus on information security. Respondents stated that they are not in a position to identify their knowledge assets.
CHAPTER 6

6. RESULTS ANALYSIS

In this section, the organisations’ perceptions of knowledge security are analysed through a theoretical framework presented in chapter 3, and the analysis is based on the data presented in chapter 5 (empirical settings and data).

6.1 On the Knowledge Security Categories and Content

In the theoretical framework of the study, it has been stated that for an organisation to have an optimal security program in place, it must address the people, the product, and the process aspects of knowledge management, and failure to protect all three will result in an incomplete program. In this section, the organisations’ perceptions towards protecting knowledge assets in these categories and their contents are being studied. And in order for time and context dependent categories and their respective content to emerge, data was iteratively analysed as described in the analysis plan. Each interview script was analysed for statements and expressions that I interpreted to reflect the organisations’s perceptions towards securing knowledge as a product, process, and the people.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Code</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>What’s the difference between codified knowledge and information? If codified knowledge is the same as information, then why do you want to refer to it as knowledge rather than information?</td>
<td>The Product</td>
<td>The statement reflects that the respondent do not understand the concept of knowledge codification but rather, they want it to be referred to as information.</td>
</tr>
<tr>
<td>I won’t say we have a way of codifying knowledge within the organisation. Why would we do</td>
<td></td>
<td>The statement suggest that the respondents does not have any means of extracting tacit knowledge</td>
</tr>
</tbody>
</table>
that anyway since we have documents that describe every detail about our systems saved in our intranets?

Oh yes, we sometimes jot down some notes when we have someone from outside talking about something we don’t know....

The respondents stated that knowledge codification is rarely done if ever it is.

We use markings such as top secret, confidential, and for official use only, to classify our information documents.

Well, listening to how you explain knowledge security makes me realise that we do have it here, it’s only that we are not aware that we have it and it’s not well defined and integrated in our policies.

The respondents stated that although some of their documents contain classified information, such documents into explicit forms and does not even see the purpose of doing so.

The statement reflects that the respondents recognise the importance of codifying knowledge, but their only way of doing so is through jotting down notes.

This reflects that if ever there is knowledge codification here, there is only a little of it and the respondents are not even sure if that little codification do happen.

The statement reflects that the organisation understands the purpose of tagging knowledge documents in securing such knowledge assets.

The statement reflects that even though they were initially un–aware that to some an extent they had something to do with knowledge security, they now recognise that they do have it.

The organisations do not understanding the importance of tagging documents in securing them, and they believe keeping them in...
are not tagged, and they stated the reason for that is they know that such documents are kept in highly secured places.

<table>
<thead>
<tr>
<th><strong>As far as I’m concerned, knowledge is what is in someone’s head. How do you secure something in someone’s head?</strong></th>
<th>The people</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>We are not in a position to identify all knowledge assets in our organisation. For us to do that, first you will have to enlighten us on what entails knowledge assets and what not.</strong></td>
<td>The Process</td>
</tr>
<tr>
<td><strong>We rely on our security policies, training and awareness programs to make sure that people do the right thing.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Our people by default know what to share and what not to share.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>This statement reflects that the respondents do not see the possibility of securing knowledge that is carried in their employees’ heads.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>The statement reflects that the respondents do not know what are knowledge assets.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>The statement suggest that the respondent has only one way of dealing with people in protecting knowledge assets, and this is through policies and security trainings.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>This is an assumption by the respondents that the employees know critical information and knowledge assets they are not supposed to disclose to the public.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Well, even though we don’t have anything to do with the protection of knowledge generation processes, we</strong></td>
<td></td>
</tr>
<tr>
<td><strong>The statement suggest that even though they don’t have formal methods on how to protect the processes of knowledge generation,</strong></td>
<td></td>
</tr>
</tbody>
</table>
believe that our policies, training and awareness programs can protect the processes of knowledge generation in our organisation.

We rely on the security technology that we have to make sure that our operational processes are kept safe.

The respondents find the importance of doing so, and they believe somehow their policies and training programs can help them in that area. It shows that the the organisation haven't yet established formally the methods for protecting the processes of knowledge generation.

The statement reflects that apart from security technology, they don’t have any means of making sure that their processes are safe.

The categories of the data coding was influenced by the theoretical framework of the study, and it was important to understand the basic differences between the categories since protecting knowledge assets through those categories is often applied differently. It was also important to find all the statements that reflected the organisations’ perceptions of securing knowledge assets in those three categories. After careful selection of those statements, it then became apparent that the respondents’ statements showed some patterns and I then used (Miles & Huberman, 1994)’s pattern coding to find inferential patterns from each organisation’s coded data (table 2).

**Table 2 Emerged Data Patterns**

<table>
<thead>
<tr>
<th><strong>The Product, People, and Process</strong></th>
<th><strong>Patterns</strong></th>
<th><strong>Interpretations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisations believe that information that is kept as documents cannot be referred to as knowledge, but they find knowledge to be something in someone’s head.</td>
<td>In-ability to understand knowledge forms</td>
<td>This pattern actually tells us that the basic reason why organisations state that they don’t have anything defined as knowledge security is because they don’t realise that the same information</td>
</tr>
<tr>
<td>The organisations find knowledge security as a very difficult thing and they are not sure if its something they will implement in their organisations</td>
<td>Readiness to implement knowledge security</td>
<td>The statement reflects that as long as organisations are not making any efforts to understand knowledge security, to see it being implement soon can only be a dream and as such knowledge assets will continue to be vulnerable to compromise.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Organisations believe that by jotting down notes during presentations is enough as a way of codifying knowledge.</td>
<td>In-ability to use other knowledge codification methods</td>
<td>The statement reflects that majority of knowledge carried by the employees is never capture and stored safely as explicit knowledge which means any employees who want to leave the organisation will also leave with the valuable knowledge they have and consequently a big loss to the organisation.</td>
</tr>
<tr>
<td>Organisations rely heavily of the security technology they have such as firewalls and intrusion detection systems to make sure that their operational processes are safe</td>
<td>Over reliance on security technology</td>
<td>The statement reflects that some of the knowledge communication channels that cannot be monitored through security technology such as face to face communication are</td>
</tr>
</tbody>
</table>
The data showed that the leadership in organisations are more concerned about guarding viruses from entering the networks and the theft of equipment, and they are doing very little in educating and motivating the employees on protecting their knowledge assets.

| Role of leadership | The statement reflects that the little effort displayed by the leadership in guiding their subordinates means the success of protecting knowledge assets will be hard to be realised. Leadership need to give direction and foresight. |
| Selective provision of training and awareness programs | This reflects that there is lack of proper management in sensitising users on how to handle sensitive information, and this reflects a very big loophole as users are often the weakest link in security. |
| Un-signed security policies | This reflects that in any case an employee have a breach of conduct, the organisation may not hold such person liable because such person has not signed any policy and there is no proof that he |

Although all organisations have security policies in place, data showed that such policies are never signed the employees and some employees are not even aware of availability of such
policies was even aware that this was a breach of conduct.

<table>
<thead>
<tr>
<th>The organisations stated that they always try to retain their staff by motivating them with more incentives such as pay rise and better working conditions, and if such incentives are not enough then they have no choice but to let such people leave.</th>
<th>Motivation to retain staff</th>
<th>This reflects that organisations find the importance of retaining staff in securing their knowledge assets and they are motivated to do so. This shows a good move in the right direction in securing knowledge assets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is knowledge security anyway?</td>
<td>Understanding of the term knowledge security</td>
<td>These expressions reflect that not all people understand what is knowledge security and if it's something possible in their working environments.</td>
</tr>
<tr>
<td>Man, what is that? Is it something we can do here?</td>
<td></td>
<td>The statement reflects that the respondents were initially not aware that in some quarters they have knowledge security but now they realise that they do</td>
</tr>
</tbody>
</table>
While some organisations indicated that they do tag their knowledge assets, others showed they don’t do so and they don’t see the importance of doing so if their knowledge assets are kept in secure places.

<table>
<thead>
<tr>
<th>Differences in perceptions towards knowledge assets tagging</th>
<th>This reflects that different organisations may perceive different situations differently hence use different approaches to secure their knowledge assets</th>
</tr>
</thead>
</table>

have. This was actual the result of lack of understanding what knowledge security is.
CHAPTER 7

7.1 DISCUSSIONS AND CONCLUSIONS

The focus of the study was to find out how different organisations around Botswana protect their knowledge assets. The premise of the research was that, even though protecting knowledge can be such a problem, the organisations understand the criticality played by these knowledge assets in giving them the competitive advantage, and as such they would devise some methods to make sure that these knowledge assets are protected and not accessible to the wrong people. Up to this point, I have articulated and analysed different methods applied by these organisations in protecting their knowledge assets. A couple of researches have been done in the past about how organisations protect their knowledge assets, for example, (Desouza & Vanapalli, 2005), but they specifically focus only on the often so called sensitive and strategic departments such as defence and security, financial sectors, while few focused on all organisations in general. Such approach has led to the lack of appreciation by other organisations that knowledge security is an important concept to all, and not just for the so called sensitive departments.

Although most of the current literature, e.g. (Desouza, 2007), (Nonaka & Takeuchi, 1995), (Liebeskind, 1996) etc. tell us how to protect knowledge assets in an organisation, they don’t really tell us why most organisations do not have proper methods of protecting these assets. It can be said that one contribution this research brings to the current literature of knowledge security is why most organisations are left behind in securing their knowledge assets. Through this research, it has been revealed that the surveyed organisations do not appreciate knowledge security not because they chose to do so, but mainly because they know very little about it. It is therefore through this research that it was found that organisations need be sensitised more about knowledge security before they can be expected to effectively secure their knowledge assets.

Looking in details the results of the research, it can be seen that it is not entirely true that the organisations have nothing to do with knowledge security like they say. The research has been revealed that in-deed organisations have knowledge security in some way but they are not aware that what they are doing is part of protecting knowledge assets. The fact that they said they have nothing to do with knowledge security is more attributed to their lack of
understanding of what knowledge security is. For example, some of the patterns revealed by the research analysis showed that after thorough explanations to them, the respondents started to realise that in fact they do have knowledge security but because it was not well defined and well documented in their policies, they were not aware of it. Organisations argued that they don’t know what codified knowledge is, and they only understand it if it’s referred to as information. However, (Al-Hawamdeh, 2002), agreed that indeed explicit knowledge is information. Thus, explicit knowledge, codified knowledge, or knowledge as a product can be used to refer to information. Because all organisations have information security policies, we can conclude that all organisations have some of knowledge security policies despite the fact that they don’t call it or understand it as knowledge security.

(Desouza & Vanapalli, 2005), argued that for an organisation to have an optimal security program in place, it must address the product, the people, and the process aspects of knowledge management, and failure to do so will lead to an incomplete security program. However, this research has revealed that in fact, the surveyed organisations are not even aware of knowledge forms (i.e. tacit and explicit knowledge). This un–awareness of knowledge forms actually means these organisations cannot categorise their knowledge as either product or people because they are simply un–aware of it. This will then mean their security program cannot address all the aspects suggested by (Desouza & Vanapalli, 2005), hence an incomplete security program. In other words, this research adds to (Desouza & Vanapalli, 2005) by suggesting that for organisations to have a complete security program, first there should be a clear understanding of different knowledge forms, and this will then lead to categorisation of knowledge as a product, people, and the process. Because knowledge security was never made part of their mandate in the first place, the surveyed organisations find it a very difficult to understand what knowledge security is, and as such they find it as something they are not ready to implement yet. This however, does not necessarily mean they do not find it important to them or they don’t have knowledge assets to protect, because it was also found through this research that when explained, the organisations appreciated the importance of knowledge security towards their competitive advantage. (Nonaka, 1994)’s dynamic theory holds that organisational knowledge is created through a continuous dialogue between tacit and explicit knowledge……… (Nonaka & Takeuchi, 1995), also argued that organisational knowledge creation should be understood in terms of a process that organisationally amplifies the knowledge created by individuals and crystalizes it as part of the knowledge network of the organisation. Thus, knowledge in an organisation is created by individuals. What can be understood from these statements is
that knowledge is always present in an organisation. And when thoroughly explained to them, organisations showed appreciation that knowledge security is indeed an important concept for them also. But the fact that they don’t have enough knowledge about it, they find it as something they cannot manage to do at the moment.

Employees are one of the most valuable knowledge assets in any organisation because of the knowledge they carry in their heads. This actually means when they leave, the organisation faces one of the critical situations, and remedies are needed to minimise the effects of the loss. One of those remedies is codifying the knowledge they carry so that when they leave, the knowledge they possess is left behind. However, this research has revealed that the surveyed organisations depend on note taking (often known as jotting down notes) as a way of doing their knowledge codification. Jotting down notes in simple terms mean doing in small amounts. This means there is little codification done in organisations to compensate for departing staff, and as such a lot of knowledge is lost when staff leaves for greener pastures. This actually confirms with (Desouza & Vanapalli, 2005) that unlike DIS and Intelligence sectors, documentation in organisation comes as an afterthought. This is probably one of the reasons why DIS and intelligence sectors enjoys the success of protecting knowledge assets, due to the saliency they put on documenting everything, while other organisations don’t enjoy the same success. However, all is not lost when individuals leave the organisation. (Nonaka & Takeuchi, 1995), describe socialisation (conversion of tacit knowledge to another tacit knowledge) as the process of sharing experiences, thereby creating tacit knowledge such as mental models and technical skills. This is where an individual can acquire tacit knowledge directly from others without the use of language, and this is made possible through observation, imitation, and practice.

The research also revealed that another good reason why organisations are lacking behind in knowledge security is the role played by leadership in protecting these knowledge assets. Unlike (Desouza & Vanapalli, 2005), revealing that leadership generally should be at the forefront of anything that happens in the organisation, and that the mandatory usage of knowledge management systems should be ordered by the leadership, this research reveals that in fact leadership in the surveyed organisations are more concerned with viruses entering their networks and the theft of their equipment. The research revealed that because of lack of knowledge about knowledge security by the leadership, the protection of knowledge assets within the organisation have received very little attention not only from the lower level staff but also from the leadership. This lack of attention given to the protection of knowledge assets by the leadership in organisations means these knowledge assets are more likely to be compromised hence organisations face disastrous consequences.
(Desouza & Vanapalli, 2005), argued that the prime reason why DIS and Intelligence sectors have gruesome training and indoctrination process is to make sure that only the people who meet the highest standards in terms of ethics, training, and knowledge are retained. This is however, as revealed by the research, is in opposite with the current practices in the surveyed organisations, and probably explains another reason why these organisations do not enjoy the same success as DIS and Intelligence sectors in protecting their knowledge assets. The research revealed that organisations provide their security training selectively, as not all employees in organisations have received such trainings. This kind of setback has been indicated by most researches in the past that providing security training to only a section of the employees cannot do any good to the security of the organisation.

The research has shown that organisations put huge reliance on security technology to protect their assets. One of the commonly stated comments were; “we have powerful firewalls and intrusion detection systems to protect our assets from any harm”. But, knowledge is communicated through channels, and some of these channels e.g. face to face communication has proven to be extremely difficult if not impossible to monitor through technology. However, despite literatures such as (Desouza & Vanapalli, 2005), indicating that strict security protocols such as those used in DIS organisations can be used to alleviate the situation, this research revealed that surveyed organisations however, still believe that security technology is enough to protect their communication channels. This rather, shows that knowledge assets in these organisations are more likely to be compromised through communication channels such as face to face communication due to lack of proper mechanisms in place to make sure that all communication channels are safe to channel knowledge assets.

Not all weaknesses shown by the organisations in securing their knowledge assets can be blamed on the lack of knowledge about knowledge security. Some of the weaknesses revealed by this research have shown that they are more attributed to incompetency. For example, the research revealed that when employees sign new contracts of employment, security policies were never made available for signing let alone being brought to the attention of the employees. Organisations always keep their policies on their intranets and assume that the employees are aware of them. However, the research revealed that most employees are not even aware that such policies do exist. This is despite the fact that organisations know very well the importance of signing security policies and making sure that everyone who signs the policy understands the contents of the policy. But still after
knowing all that, the organisations never made such policies available for signing or even make sure that the employees are aware of them, which is a sign of incompetence in the workplace. This can be described as lack of dedication towards making sure that the organisation’s assets are safe and secure from any harm.

The surveyed Organisations have shown that they understand the importance of keeping their staff so that they do not lose the knowledge they have, and they offer incentives such as pay rises, good working conditions, and other bonuses such as car and house allowances to make sure that valuable staff is motivated to stay on with them. This is agreement with literature e.g. (Liebeskind, 1996) that by providing credible long term incentives, a firm also increases the incentive for an employee to invest in a formal personal relationships with other employees, thereby increasing the likelihood that an employee will become emotionally attached to other employees or to the organisation as a whole, and this attachments will also increase the employee’s cost of exit. The incentive theory of motivation also posits that environment brings behaviour, if goals are present people will want to reach to those goals, and the behaviour is shaped by profitable intent. This shows that for the organisations to be giving more incentives to retain staff, they are in actual fact doing what the current literature suggest, hence a move in the right direction.
7.2 RECOMMENDATIONS

This section proposes the recommendations for securing knowledge assets in organisations around Botswana. It utilises the lessons learned from Defence and Intelligence Sectors by (Desouza & Vanapalli, 2005) to build on the proposed framework. (Desouza & Vanapalli, 2005) stated that for an organisation to have an optimal security program in place, it must address the people, product, and process aspects of knowledge management. And as such, the recommendations provided here are based on such argument. Also, past knowledge security researches that were outlined in the theory chapter were also utilised to add in the building of the proposed framework, in order to suite the situation present in the surveyed organisations. The recommendations were presented based on the results supported by the data in each level. It is worth noting that the recommendations provided are not arranged in any particular order.

THE PRODUCT

Here the focus is on securing knowledge that is already in codified form. Although the organisations stated that they don’t have knowledge security in their organisations, the research revealed that such assertions are not true. (Nonaka, 1994)’s Dynamic Theory of Organisational Knowledge Creation holds that knowledge assets are always present in an organisation. But the research revealed that the surveyed organisations are not aware of these knowledge assets and the practices needed to protect these assets. I then propose the following points when considering security of knowledge as a product.

Identify Valuable Knowledge Assets. From an organizational perspective it is important to be specific in determining what organizational knowledge truly represents intellectual assets. Different knowledge assets have different values attached to them, and some don’t need to be secured as they are invaluable. Not all knowledge that an employee has can be put in use. Therefore, the organization cannot afford to provide security to all explicit knowledge that exists within the organisation. (Desouza, 2007) discussed a framework for identifying intellectual assets in an organization. He stated that any asset needs to have value. Value emerges when we put an asset in use, and in order to use an asset, one must have the necessary capabilities and intent. In this content, necessary capabilities come down to having the organizational process required to take an advantage of the asset, while intent is the strategic direction and focus of the direction. Once we determine that in fact the
resource contribute value, the next question to ask is what kind of value does the resource have? (Desouza, 2007), stated that at the basic level, a knowledge resource should contribute to the operational effectiveness and efficiency of the organization. The next question to ask would be what is the future value of the asset? That is, is it an increasing or decreasing value? Unless an asset has future potential, the cost one will incur in securing it will be unjustified. Once we have ascertained that a given resource contributes value to the organization, the next question to ask is how rare is the resource? A resource that is not rare to find may be easily replaced, hence the cost of securing it may be unjustified. (Desouza, 2007), stated that the lack of rarity is commonplace when we consider knowledge resources that contribute at operational level. Knowledge resources at the strategic and tactical levels are more likely to exhibit the characteristics of rareness. The next question to ask is, is the knowledge resource non-imitable and non-substitutable? Non imitable means the knowledge resources cannot be duplicated, at least not at a reasonable cost and/or effort. The cost of securing knowledge resources that are easily imitable and substitutable may well not be justifiable. (Desouza, 2007), stated that knowledge resources that are non-imitable and non-substitutable, in addition to being valuable and rare, need to be given the outermost care, as they are the highest valued intellectual assets of the organisation.

In summary, the questions you need to ask yourself when identifying intellectual/knowledge assets in your organisation, as suggested by (Desouza, 2007) were:

1. Is the resource or capability valuable?
2. Is the resource or capability rare?
3. Is the resource or capability non substitutable?
4. Is the resource or capability non imitable?

If the answer is yes to all questions, the resource or capability is an intellectual asset of the highest value. If the answer to question 1 is no, the resource or capability is not an intellectual asset. If the answers to question 3 and 4 are no, the resource or capability might be an intellectual asset depending on the context of the organisation, of they could be assets of a lower value.
**Document all Valuable Knowledge Assets.** The dynamic theory of organizational knowledge creation holds that indeed knowledge can be extracted from individuals and be made explicit (documented) through a process known as externalization. Externalization is a process of articulating tacit knowledge into explicit concepts, where tacit knowledge becomes explicit by taking forms of metaphors, analogies, concepts, hypothesis, or models (Nonaka & Takeuchi, 1995).

Whether the goals for a community include preserving, protecting, or sharing knowledge, it is becoming increasingly important to record and document this knowledge, said (Hansen & VanFleet, 2003). Documentation is fundamental to both preserving this knowledge for current and future generations, as well as protecting intellectual property rights. (Christensen, 2003), stated that knowledge management must also consider strategies for retaining knowledge as a consequence of the fact that human resources constitute the company’s most important resource. Retaining knowledge is thus a question of ensuring that the knowledge possessed by the employee is not lost but it must also ensure that the knowledge retained is the right knowledge– valuable knowledge.

Now the point is, can tacit knowledge actually be documented, and if yes, how? (Nonaka & Takeuchi, 1995), stated that the answer to how can we convert tacit knowledge into explicit knowledge effectively and efficiently, lies in the sequential use of metaphors, analogies, and models. (Christensen, 2003) states that although under the right conditions and with the right help we can make quite a lot of tacit knowledge explicit, not all tacit knowledge can be made explicit, and as a result, the process of documenting knowledge must be controlled so as not to waste too much time in documenting something that cannot be documented. But then, how can we document something that cannot be identified? (Christensen, 2003), stated that documentation of tacit knowledge need not necessarily as so epistemically bewitched. The point of departure when comes to documenting knowledge ought rather to be that perception-based knowledge usually can be documented explicitly in e.g. databases, whilst tacit knowledge can be documented in relations between individuals or in individuals trained by the person who possesses indispensable (tacit) knowledge. Thus, the documentation of knowledge requires time; time for qualifying knowledge, time for the keying in of knowledge, and time for the transfer of knowledge between individuals. Transfer of knowledge will also presents some number of challenges concerned with
whether people wish to allow their tacit knowledge to be documented through e.g. mentoring arrangements. (Christensen, 2003) states that when documenting knowledge, it is also important to ensure that what one is documenting is actually knowledge. This makes demands on companies to set up epistemic criteria for what makes something knowledge, and if it’s valuable knowledge. This actually justifies the point (above) that before documenting knowledge assets; you need to determine if they are truly knowledge assets that have a degree of importance to the organization.

Segment Documented Knowledge.

Some of the surveyed organisations indicated that they don’t see the importance segmenting and tagging of their knowledge assets if they are kept in safe places. But segmenting knowledge helps in the classification of documented knowledge. (Desouza & Vanapalli, 2005), stated that similar to the clearances for employees, documents are segmented by security clearances and markings. Documents are marked by notations such as confidential, classified, secret, top secret, internal, or public. These notations ensure that the knowledge presented in the document is controlled in terms of who might have access to it. Only organizational members who possess the necessary security clearances can be privy to material that is of a given sensitive level, said (Desouza & Vanapalli, 2005). Although local organisations have a way of classifying their documents, very few do so, and that actually impact negatively on security of their stored documents.

THE PROCESS

On Identification and authentication

Upon reflecting on why DIS organisations are very successful on protecting their knowledge assets, (Desouza & Vanapalli, 2005), stated that an agent must always identify themselves before getting access to the knowledge process. Identification mechanisms enable a user, device or a process to present its credentials to a system. They state that in armed services, identification takes the form of seeing the badge and the stripes worn by the person you are engaging in conversation with. Following strict identification and authentication protocols will usually help in alleviating the chance of disclosing sensitive
data or secrets of the organisation to competitors or intruders. All individuals within the
organization should follow these strict rules to avoid putting the organisation in danger.

Authentication results in positively verifying the identity of a user, device, or another entity
in an information system. This is often a pre-requisite for allowing access to resources
offered by the system (Gattiker, 2004). He states that in an area of high risk, stronger
authentication may be required such as asymmetric keys, biometrics, cryptographic tokens,
digital certificates, smart cards, and one-time password generators. (Gattiker, 2004), also
stated that strong authentication relies on combining one or more of the following.

- Password/ pin or something the user knows
- Token or other means, that is something the user has, and finally
- Biometrics or other technique enabling the system to identify who the user is.

Also, a lot of information security literature has more details about authentication and
identification mechanisms, and if organizations can review such literature, they can come
up with more suitable methods for them. Although different literature explains
identification in terms of information security and not knowledge security, I find their
applications similar between the two concepts; hence all information security literature that
talks about authentication and identification will also apply to knowledge security.

**Prioritise your Goals**

There are many knowledge security goals that an organisation may want to achieve, and no
organisation can be able to attain all of them at the same time. The attainment of these goals
may be limited by several factors such as budget, service provision to the clients, and other
factors that are beyond the control of the organization. So, to achieve the knowledge
security goals in an organization, prioritisation of these goals will play a big role.

(Desouza, 2007), stated that no security budget will be adequate, nor will you ever find an
organization devoting ample resources to security. Given that you will never be able to
secure all the intellectual assets in an organisation, you must prioritise where to spend your
energies, (Desouza, 2007). Not all intellectual assets are the same in an organization, and
not all the employees are the same. Some are actually highly valuable than the other.
(Desouza, 2007), stated that the most highly valuable employees need to be protected first; then you can move to the rest. Not only valuable employees need to be given priority when protected, but also to all other knowledge assets that satisfies their highest value. The loss of some assets, though painful, can be tolerated, while there are some assets that need to be secured at all costs; as failure to do so can results in an organisation collapsing.

**Secure Knowledge Communication Channels.**

Some communication channels can easily be secured using traditional security technology, but not all can be monitored using that technology. The huge reliance on traditional security technology by the surveyed organisations put them on a more vulnerable situation. For example, how would face to face communications be monitored using traditional security technology? This is certainly a challenge to most organisations. Securing face-to-face communication requires a change and monitoring in the attitude and behaviour of individuals. (Desouza, 2007), stated that protecting cooperate knowledge has more to do with people than it does guards and technology. So, organisations need to put more emphasis on changing the attitude and behaviour of their individuals in order to make sure that face to face communication is secure. (Wilson & Hash, 2003), stated that in a situation where you have to deal with people factor rather than technology factor, a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organisational policies, and how to properly use and protect the IT resources entrusted to them. Making staff aware of the risks and their responsibilities helps them act in a sensible and secure manner

**On Leadership Roles**

Organisations need leadership at all costs, from top to bottom. At the top, leaders make the broad, comprehensive, and strategic decisions that set the organisations long term direction, said (Zand, 1997). They determine the character of the product line– the range of features, the quality level, and the degree of innovation. At the lower levels of the organisations, first and second level supervisors manage the firm’s day to day operations. They translate strategy into action. They see that work gets done, products are delivered, and customers are satisfied. Their leadership greatly affects the attitudes and the productivity of workers. Thus, the incompetency of the organisations towards securing knowledge assets revealed by the
research can be blamed on their leadership. Leaders in organisations should influence knowledge security at all costs for it to be granted any success. The incentive theory of human motivation posits that people can be made to be what you want them to be, as long as the right environment is created around them. It is the role of the leadership to create that environment around individuals within the organisation, and an example of how such environment can be created is instilling security culture among them. Knowledge resides in people’s heads, and people cannot be forced to do certain things with the knowledge they possess. One of the best methods securing knowledge in people’s heads is by making knowledge security a social norm within the organisation. By making knowledge security a social norm, people won’t feel they are being forced to do things they don’t want but rather they will take it as a way of living. (Liebeskind, 1996), also noted that firms can influence employees’ attitude in numerous different ways, such as advocating certain personal values or attitudes (e.g. loyalty to the firm), and providing social rewards to individuals who demonstrate certain desirable behaviours (e.g. maintaining confidentiality), and attempts to influence attitudes are more effective, the longer an individual is exposed to them, and the less that individual is exposed to countervailing influences. It is actually the role of leadership to see that knowledge security becomes a social norm between individuals in an organisation. (Tipton & Krause, 2003), also noted that the security director has the responsibility of promoting education and awareness as well as staying abreast of the new developments, threats, and countermeasures (Desouza & Vanapalli, 2005), came up with some of the roles leadership should play in securing knowledge assets in an organization. First, mandatory usage of knowledge management systems should be ordered by leadership. They state that knowledge management systems are not optional tools; they are critical components of work practices, decision making, and task assignments. Second, leadership must seek to integrate the different functions of the organisation. They communicate with their subordinates, who then must relay the information to their subordinates, and so on until the message is passed on. This communications should be clear, frequent and open to all staff members. Leaders should also focus on ensuring goal conformity. The organisations missions are put at the forefront and all are asked to rally behind them. (Desouza & Vanapalli, 2005), stated that just like we would hold an employee accountable for stealing office property, we must begin to hold people accountable for the intangibles. It is important to ensure the people are
held accountable in how they utilise organisational knowledge in the pursuit of tasks and assignments.

THE PEOPLE

Build a Security Team

Security is not a one man’s job. Building a security team is critical in the success of protecting your knowledge assets, and (Desouza, 2007), identified it as another strategic consideration when securing knowledge assets. He states that individuals who make up your security team are the most important assets in the defence against intellectual assets breaches and sabotages. This team should have the most desirable characteristics. First each individual should display the outmost integrity and allegiance to the organization. (Desouza, 2007), stated that security professionals are called upon to conduct difficult assignments. These assignments may require them to access sensitive material, and will normally involve some ethical questions. In these situations, it is absolutely essential to use individuals who work with the highest level of integrity, and in the same vein, only individuals who display unfettered allegiance to the organisation can be used. Secondly, the security team should be comprised of individuals with a wide assortment of skills and capabilities. Having only techno-geeks in your team is not sufficient, even if 90 per cent of the threads in an organization arise from technology centred attacks, (Desouza, 2007). Thirdly, the security team will compromise of individuals with a variety of experiences, and experience in this case translates to the previous work experiences. (Desouza, 2007), stated that it is good to build a team of people who are not going to engage in group thinking because of their similar backgrounds. The other dimension in experience is age, gender and cultural background. The novices, with their curious natures, may be able to challenge invalid assumptions held by experts. Fourth, the security team must be a cohesive unit. It is important for the culture of the security team be unifying, binding, open and warm. Security teams may have difficult tasks to accomplish at times, and the varying culture of the team should not be a disrupting factor. Finally, security team should be paid well, (Desouza, 2007). He states that if you want your security personnel to build an allegiance to your organization and protect your assets, you must provide them with necessary remuneration. The incentive theory of human motivation also posits that people are driven by goals, and if the goals are in place, they will try to reach those goals. Goals in this case
are remuneration provided upon securing intellectual assets. (Liebeskind, 1996), also agrees with above sentiments that by providing credible long term incentives, a firm also increases the incentive for an employee to invest in a formal personal relationships with other employees, thereby increasing the likelihood that an employee will become emotionally attached to other employees or to the organisation as a whole, and this attachment will also increase the employee’s cost of exit.

**Categorize your Employees**

Just like it is stated in the above section (prioritise your goals), the most highly important employees in an organization need to be protected first, and more attention should be directed to them. Even though it might not sound politically correct to say; not all employees in an organization are the same in terms of value and importance, the truth of the matter is they are not, and they will never be. Some employees within the organisation are more valuable than others, and some possess some skills that are not readily available within the rest. If an employee possesses knowledge and capabilities that are rare, non-imitable, non-substitutable, and are of value to the organization, then the organisation needs to pay attention to him or her and ensure that there are adequate mechanisms in place to protect the person’s knowledge (Desouza, 2007). In this case, it is advisable to group people who possess that valuable knowledge together, and also those who possess less valuable knowledge together. By doing so, it can help the organisation in managing and protecting most valuable and sensitive knowledge that employees has. Identifying and categorising employees based on the value of the knowledge they have shouldn’t be a difficult task, assuming the organisation follow the suggestions provided above (identifying valuable knowledge assets).

**Instil Security Culture**

The surveyed organisations indicated that they are not aware of what knowledge security is, and they are not in a position to implement it. The research also indicated that although security policies and training programs are available within the surveyed organisations, they are rarely availed and selectively implemented within the organisation. Unlike providing selective training to your employees like the surveyed organisations do, all actors in the knowledge economy of the organisation have to be given proper security training.
NIST Special Publication 800-50 indicates that a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organisational policies, and how to properly use and protect the IT resources entrusted to them. Because the surveyed organisations rarely avail security policies and training programs to all their employees, it might also be impossible for them to hold accountable those who break the rules.

(Garrett, 2004), noted that the challenge to many organisations is to create a security-aware culture. To shift the cultural paradigms of organisations into a mode where security becomes inherent requires changes in the structure of the cultural web, and a critical additional factor in achieving real cultural change is in changing the behaviours of individuals throughout the organisation to support new policies, procedures and structures. The Incentive theory of motivation posits that the incentives shape the behaviour of individuals. These incentives do not need necessarily be monetary, but they can be non-material forms like love, respect, or even punishment. If incentives are used, people will change their behaviour towards securing their knowledge assets.

(Desouza & Vanapalli, 2005), stated that DIS organisations are in fact obsessed with making sure that only the people who meet the highest standards in terms of ethics, training, and knowledge are retained, and this is the prime reason for the gruesome training and indoctrination process associated with joining any of the armed services. In actual fact, the gruesome training and indoctrination means instilling the culture they want in their employees. This is one of the lessons that local organisations can learn from Defence and Intelligence sectors, by trying to instil knowledge security culture in their employees. People see culture as a way of living, and if they see knowledge security as their way of leaving, great success in protecting knowledge assets can be guaranteed.
The Framework

1: Identify valuable knowledge assets
2: Document all valuable knowledge assets
3: Segment documented knowledge assets

1: Strong authentication and Identification
2: Prioritize goals
3: Secure Knowledge communication channels
4: Leadership roles

Figure 4. Summary of Proposed Framework
FURTHER STUDIES

This research was conducted within the boundaries of Botswana and the results of the research might be difficult to generalise to other countries due to the diverse cultures and laws between the countries. As such, future studies may focus on applying the research on different countries so that the results be generalised across different states.

During the research of this project, there were very little theories that specifically defined knowledge security, and as such, the theoretical framework relied much on past researches from internationally well-known knowledge security researchers, and also from other knowledge management theories, to explain knowledge security. Therefore, future research can focus on finding specific knowledge security theories that can make the research stronger.

At the end of this research, recommendations have been provided to be used by organisation in protecting their knowledge assets. Such recommendations were provided in general terms. However, different organisations have different situations in the protection of their knowledge assets. In this case, future studies can focus on how different organisation can apply knowledge security given their specific situations.
REFERENCES:


a.
APPENDICES

The questions asked on the interview were designed with the guidance from the theoretical framework. The target was to get enough information from the respondents that was already outline in the theory chapter.

INTERVIEW GUIDE

Name: _____________________________________________________

Organisation: _______________________________________________

Position Held: ______________________________________________

Date: ______________________________________________________

1. Does the term knowledge security make sense to you?

2. Do you see any importance in securing your organizational knowledge assets?

3. What are the mechanisms in place right now in your organisation that you use to secure intellectual assets?

4. Are you in a possession to identify intellectual/knowledge assets in your organization right now?

5. Are you in a possession to identify knowledge assets that have been compromised in your organization?

6. Why do you think knowledge assets get compromised in your organization?

7. How do you respond to incidents relating to your knowledge assets?
8. Would you say your employees are able to identify knowledge assets within the organisation?

9. Do you have any criteria of classifying knowledge assets?

10. How do you prioritise information security in your organization?

11. Do you have any personnel specifically trained for information security? If not, do you think you need one?

12. How would you rate your information security staffing?

13. Regarding your management strategies, how do you make sure that your employees secure your intellectual/knowledge assets in the organization?

14. How do you motivate your colleagues to protect intellectual assets?

15. Do you have any knowledge security training/ awareness programs for your employees in your organization?

16. Do you have any security clearances for your knowledge assets? Clearances can be; confidential, secret, classified, etc.

17. State in brief how your security structure looks like.

18. How do you as an organisation, make sure that when staff leaves the critical knowledge they have is retained in the organisation?