THE INSTITUTIONALISATION OF AN INFORMATION SECURITY CULTURE IN A PETROLEUM ORGANISATION IN THE WESTERN CAPE

by

MICHAEL MICHIEL

Dissertation submitted in fulfilment of the requirements for the degree

Master of Technology: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Dr Andre de la Harpe
Co-Supervisor: Mr Ayodeji Olanrewaju Afolayan

Cape Town
June 2018

DECLARATION

I, Michael Michiel, declare that the contents of this dissertation represent my own unaided work, and that the dissertation has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed **Date**

ABSTRACT

In today's world, organisations cannot exist without having information readily available. The protection of information relies not only on technology but also on the behaviour of employees.

The failure to institutionalise an information security culture inside an organisation will cause the continued occurrence of security breaches. The aim of the research is to explore how an information security culture can be institutionalised within a petroleum organisation in the Western Cape.

The primary research question is posed as follows: "What are the factors affecting the institutionalisation of an information security culture?" To answer the research question, a study was conducted at a petroleum organisation in the Western Cape. A subjectivist ontological and interpretivist epistemological stance has been adopted and an inductive research approach was followed. The research strategy was a case study. Data for this study were gathered through interviews (12 in total) using semi-structured questionnaires. The data collected were transcribed, summarised, and categorised to provide a clear understanding of the data.

For this study, twenty-four findings and seven themes were identified. The themes are: i) user awareness training and education; ii) user management; iii) compliance and monitoring; iv) change management; v) process simplification; vi) communication strategy; and vii) top management support. Guidelines are proposed, comprising four primary components. Ethical clearance to conduct the study was obtained from the Ethics committee of CPUT and permission to conduct the study was obtained from the Chief Information Officer (CIO) of the petroleum organisation.

The findings point to collaboration between employees, the Information Security department, and management in order to institute a culture of security inside the organisation.

Keywords: Information security, information security culture, corporate culture, frameworks, organisational culture, human behaviour

ACKNOWLEDGEMENTS

I would like to thank God for the grace and courage granted to me throughout my research journey.

I would also like to extend my sincere gratitude to every individual who supported me throughout the duration of my study. In particular:

- My wife and two children for providing support, prayers and encouragement – I love you all
- My father, sister and brother for their support and prayers
- Dr Andre de la Harpe, my supervisor, for his diligent responsiveness, guidance and encouragement during the journey
- The reviewers, for the comments and guidance during the proposal defence and the thesis
- My employer, “Engen”, for allowing me to conduct the study

The financial assistance (URF) of the Cape Peninsula University of Technology (CPUT) towards this research is acknowledged. Opinions expressed in this thesis and the conclusions arrived at, are those of the author, and are not necessarily to be attributed to CPUT.

DEDICATION

This study is dedicated to my late mother, Clarice Michiel, who always believed in me. Today I am a product of all her sacrifices.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY / DEFINITIONS

Word/Term	Definition
Breach	"A breach is the unauthorised access or violation of an established set of norms, rules, and standards" (Liu, Musen & Chou, 2015:3).
Data breach	"A data breach is a type of security incident that involves the inappropriate usage, access, acquisition, or compromise of any sensitive, protected, or confidential data or that results in the unauthorised disclosure of an individual's sensitive personal information" (Romanosky, Hoffman & Acquisti, 2014:14).
Information security culture	"The assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics, and as the way in which things are done in an organisation" (Martins & Eloff, 2002:02).
Information security	"The preservation of confidentiality, integrity and availability of information" (Dimitriadis, 2011:43).
Policy	"Is a set of procedures that are used to be a guideline for good practice" (Thomson & Van Niekerk, 2012:44).

LIST OF ABBREVIATIONS

Abbreviation	Explanation
CCTV	Closed-circuit television
HR	Human Resources
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISO	International Standard Organisation
IT	Information Technology
PWC	PricewaterhouseCoopers
SAP	Systems, Applications and Products
CPUT	Cape Peninsula University of Technology
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
CIO	Chief Information Officer
KPI	Key Performance Indicators
PC	Personal Computers
GM	General Manager

CHAPTER 1: INTRODUCTION

1.1 Introduction

In South Africa, more than 8.8 million citizens fall prey yearly to some form of cybercrime at home or work (Symantec, 2016). In an attempt to protect the organisations against cybercrime, large investments are made in Information Technology (IT). Despite these investments, security breaches still occur from within and outside the organisations. Attackers look for new and different ways to breach the networks of organisations. In recent times, hackers began to create fake websites to attract and ask users to download and install free antivirus software from their websites. This type of attack is successful as many users download the software from the fake website, and in doing so, expose their private information (Wook, Peiying & Junjie, 2015).

Organisations invest in antivirus systems, firewalls and other technologies, as each of these systems are sold based on its effectiveness. Despite the claims of protection, organisations are still suffering from severe information security breaches (Karlsson, Astrom & Karlsson, 2015). One of the ways security breaches occur in organisations is the absence of information security policies that protect customers, networks, systems, and data (Ruggiano & Brown, 2013). Karlsson and Hedstrom (2014) agree that humans can be the weakest spot in organisational defences and become targets for cyber criminals.

Research on information security culture is being conducted in Finland, South Africa, Saudi Arabia, Australia, and Switzerland (Al Hogail, 2015; Bulgurcu, Cavusoglu & Benbasat, 2010; Knapp & Marshall, 2006; Ramachandran, 2008; Van Niekerk, & Von Solms, 2006). The research mainly focuses on attitude, behaviour, and adopting the Schein Model (Al Hogail, 2015; Fichman 2011; Oost & Chew, 2007). Technical controls do not guarantee a universal solution to all human blunders (Karlsson et al., 2015). Irrespective of how sophisticated technologies are, losses will continue to occur. It is important for organisations to create employee awareness of their obligation towards information security and to institute an information security culture (Tang, Li & Zhang, 2015).

The aim of this research is to explore how an information security culture can be institutionalised in an attempt to limit security breaches within a petroleum organisation in the Western Cape, with specific reference to company culture.

1.2 Background to the research problem

Organisations cannot exist without having information readily available. In order to allow business to stay secure, companies make large investments in IT infrastructure to protect the information of the organisation. It is important for organisations to guarantee that their information resources are sufficiently protected against internal and external threats. During a data breach incident in 2014, hackers successfully infiltrated an organisation's network and stole 40 million credit card numbers (Riley, Elgin, Lawrence & Matlack, 2014). Internal employees are a huge concern to information security personnel because compared to outside attackers the employees have the relevant knowledge, resources and access to the organisational environment (Vance, Lowry & Eggett, 2013).

The protection of organisational information resources is typically accomplished in conjunction with the implementation of various security controls. Security controls can be divided into different categories: technical, operational, and physical controls (Van Niekerk & Von Solms, 2003:2). Technical controls refer to the technical side of information technology. For example, all computers on the organisational network should have antivirus software installed to be protected from viruses and malware infections. Operational controls refer to the daily activities taking place in an IT department, which include the monitoring and fixing of security incidents at the organisation. Physical controls refer to the physical side of security. An example of this is where an organisation invests in security guards to monitor who is entering and leaving the company premises. All employees have an important function to fulfil in order to secure organisational information resources (Karlsson et al., 2015). However, even after security awareness training programmes, employees still fall victim to phishing, social engineering, and other attacks. This is a major concern for organisations in the management of information security, as employees continue to remain a risk (Karlsson et al., 2015). The International Standard Organisation (ISO) requires that all employees of an organisation receive appropriate information security training (ISO, 2013). This training should include security awareness and other security related training. However, the ISO standard does not provide any guidance as to how this security training should be done in the organisation.

According to Schein (2009), a large volume of knowledge exists in management sciences regarding organisational culture in general, but very little is known regarding the applicability of this knowledge to information security. It is however clear that a user education programme will have to play an enormous role in the creation of such a culture (Chen, Ramamurthy & Wen, 2012). Information security culture, as defined for the purpose of this research study, stems from Schein's

model of organisational culture, where Schein (2009:21) defines organisational culture as “existing on three levels, namely artefacts, espoused values and shared tacit assumptions”. Van Niekerk and von Solms (2010) agree with the three levels of Schein (2009), however, they include a fourth level, namely information security knowledge specific to information security.

The research case used is a petroleum organisation in the Western Cape, South Africa. In this organisation, the Information Security (IS) department is responsible for the information security of the organisation. The IS department works to keep the information of the organisation safe and secure. However, the department can have the best technology in place, but if the employees of the organisation do not understand the role they have to play in keeping the information safe, they can be used as victims of cybercrime.

The purpose of creating an information security culture is to ensure that employees understand how to protect the information of the organisation. Information security is dependent on the behaviour of humans in order to be effective (Karlsson et al., 2015). Knapp and Marshall (2006) propose a separation between information security culture and organisational culture, because each organisation is unique.

1.3 Research problem

The importance of information security inside an organisation is evident after security breaches resulted in organisational financial losses (Da Veiga & Eloff, 2010). This is supported by Sommestad, Hallberg, Lundholm and Bengtsson (2014) who state that information security is a growing concern in organisations. When security breaches occur in organisations, the security team activates an incident response plan to prepare, identify, contain, remediate, and recover from a security breach.

Information security breaches occur on a daily basis in organisations (Dunsmuir & Finkle, 2015). If an information security culture is not institutionalised inside an organisation, security breaches will continue to occur, costing the organisation reputational as well financial losses (Adler, Demicco & Neiditz, 2015). Furthermore, the lack of an information security culture contributes to organisations spending huge amounts of organisational funds, and the brand reputation of the organisation can be affected (Layton & Watters, 2014). These security breaches are a result of many factors, including external employee theft, insider threat, improper access, and disclosure of sensitive information (Chen et al., 2015; Holtfreter & Harrington 2015; Liu et al., 2015). According to Holtfreter and Harrington (2015), the internal threat of employees who leave companies’ physical records such as laptops, CDs,

smartphones and hard drives unprotected, can expose them to theft. These situations can lead to the physical loss of records by current or former employees as well as theft by others. On the other hand, if the Internet network is not properly secured with the most recent software and industry standard network data security firewall, then records are exposed to internal and external hackers.

Chen et al. (2015) state that internal employee negligence create uncertainty of what needs to be done to prevent security breaches as well as disclosure of sensitive information within the organisation. The insider threat and disclosure of sensitive information is an important contributor to breaches within organisation (Liu et al., 2015). However, according to Hafizah and Ismail (2016), there is a lack of research focused on the creation of a security culture within an organisation. The authors further state that information security should be a high priority for organisations, as they have uncovered human and organisational issues in the organisations they interviewed. They also state that cultural changes are one of the most important aspects to look at in information security, and in order to strengthen this area, a culture of security needs to be inculcated in the organisation before implementing an information security management system (ISMS) (Hafizah & Ismail, 2016).

From the above discussion, the researcher identified the research problem to be: **The failure to institutionalise an information security culture inside an organisation will cause the continued occurrence of security breaches, costing the organisation reputational as well as financial losses.**

1.4 Research questions and research sub-questions

Table 1.1 depicts the research questions (RQs) and research sub-questions (RSQs), formulated to solve the stated research problem.

Table 1.1: RQs, RSQs, methods of obtaining data, and objective of the questions

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?			
RSQs	**Question**	**Method**	**Objective**
RSQ 1.1	What are the challenges the organisation is facing when implementing an information security culture?	Semi-structured interviews	To identify the challenges the support personnel are experiencing
RSQ 1.2	What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?	Semi-structured interviews	To identify the employees' reaction towards security changes

RSQs	Question	Method	Objective
RSQ 1.3	What processes can be created inside the organisation to institutionalise a culture of security?	Semi-structured interviews	To identify new processes

1.5 Research aim

The aim of this research is to explore how an information security culture can be institutionalised within a petroleum organisation in the Western Cape.

1.6 Research objectives

1.6.1 Objective 1

- To determine the factors affecting the creation of an information security culture within an organisation

1.6.2 Objective 2

- To investigate what methods could be used by the organisation to institutionalise an information security culture

1.6.3 Objective 3

- To examine different assessment processes that could be used by the organisation when creating an information security culture

1.6.4 Objective 4

- To propose guidelines that will assist the organisation in instituting a culture of security

1.7 Conceptualisation

1.7.1 Research methodology

The research design and the methods adopted are discussed in detail in Chapter 3. A subjectivist ontological and interpretivist epistemological stance has been adopted and an inductive research approach was followed. The research strategy was a case study. Data for this study were gathered through interviews using semi-structured questionnaires. The data collected were transcribed, summarised, and categorised to provide a clear understanding of the data.

1.7.2 Research delineation

The study only focuses on instituting a security culture inside a petroleum organisation in the Western Cape. Sources of data are limited to the petroleum organisation. Only information technology security employees were interviewed.

1.8 Outline of thesis structure

Chapter 1: This chapter covers the introduction of the research, thus, it includes a general introduction as well as the research problem, aim, objectives, methodology, and delineation.

Chapter 2: This chapter covers the literature review, which focuses on an overview of information security culture and organisational culture.

Chapter 3: This chapter covers the research methodology, research approach, research strategy, data collection, data analysis, and ethical considerations.

Chapter 4: This chapter covers the results and findings and consists of two sections. Section one covers the case and interviewee demographics. Section two covers responses to the research questions, findings to the research questions, and the summary of findings.

Chapter 5: In this chapter, the themes in relation to the research sub-questions are discussed in detail.

Chapter 6: This chapter covers the conclusion and recommendations of the study.

References: Included in the reference list are the references to support the study and to acknowledge the work done by others.

Appendices: All supporting documents to validate the information included and referred to in the study are contained in the appendices.

1.9 Summary

This chapter explored the topic of institutionalising an information security culture inside a petroleum organisation in the Western Cape. The chapter commenced with a background of the problem and the research problem, where after the research questions and sub-questions were discussed. The aim and the objective of this research were stated, followed by the research methodology and research delineation. In conclusion, the outline of the thesis structure was given.

In the next chapter, a literature review will be conducted on the thesis topic.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In this chapter, existing approaches to deal with the human factor in information security are discussed. These approaches include most of the current work relating to information security awareness, training and education, or the creation of an organisational culture of information security. The reason for the analysis is to provide a comprehensive overview of the current state of methods dealing with the human factor in information security in the petroleum organisation. The reviewed literature recognises the importance of addressing the behavioural aspects of information security education as opposed to exclusively focusing on the transfer of skills and knowledge. Furthermore, current literature acknowledges the need for an information security culture, and current methods have adapted the more general definitions of organisational culture used in the human and social sciences to be specific to the needs of information security.

The literature review is done by firstly identifying keywords from the title, problem statement, research questions, aim, and objectives of the study. As literature has been reviewed, new keywords were added iteratively. Online databases such as Emerald, Google Scholar, Scopus and ProQuest from the CPUT library were consulted.

The following sections present a comprehensive overview of existing methods to deal with the human factor in information security. The sections are: i) organisational culture; ii) information security culture; iii) institutionalise an information security culture; iv) methods to create an information security culture; v) process to institutionalise an information security culture; vi) Theory of Planned Behaviour; vii) assessment of an information security culture; viii) the role of assessment in cultural change; and viii) current assessment approaches to information security culture.

Various surveys have shown that employees do not always adhere to information security policies, which is part of the reason why security breaches are on the rise (Ponemon, 2016). A survey conducted by PWC (2016) has been revealed that employees target inside organisations, and that this is a reason for some security incidents. The non-adherence of employees to information security policies and procedures can be attributed to various reasons, including that employees do not comprehend the importance of adhering to security policies and procedures as well

as the risk caused by this non-compliance. Furthermore, information security seems not to be a main concern for employees, and some employees simply do not care.

Employees most likely ignore or bypass security controls if these controls impact on their work, in which case employees will choose their own goals or what is important to them over the security goals of the organisation (Beautement, Sasse & Wonham, 2008). It is thus important that employees receive adequate training and education on security risk so that they become security assets instead of liabilities to the organisation. Information security training that includes security awareness programmes will provide the employees with knowledge on information security risks.

Creating an information security culture implies instilling security as a way of life and integrating security into the behaviour and attitudes of employees to bring about a security conscious state (Ngo, Zhou, Chonka & Singh, 2009). In addition, it is imperative that an information security culture is continuously maintained to ensure its continued consistency with the organisation's goals and objectives. To this effect, it is essential to assess the information security culture periodically. Schlienger and Teufel (2003) indicate that an information security culture may be regarded as a subculture of the organisational culture. The next sections provide an overview of organisational culture.

2.2 Organisational culture

Organisational culture refers to the system of shared beliefs and values that develops within an organisation and that guides the behaviours of its employees towards essential suitable patterns of social systems that form coordinated behaviour to survive in a dynamic environment (Schein, 2009:37). Tipton and Krause (2007) believe people behave in certain ways depending on their feelings, knowledge or instincts. Security awareness programmes may provide knowledge to employees, but these programmes do not always influence their feelings or instincts about their obligations to protect information or their deeper security intuitions. This, can lead to a disconnect between the company's security policies and employees' behaviour. For example, employees will open any emails even if the emails come from strangers because they are not thinking or have not been trained about the potential security risk of opening a suspicious email.

Another example is when employees bring memory sticks containing data from home and copy the data to their work computer without thinking about the effect this can have on the company's network. To close this disconnect between the user's

behaviour and what is required from an information security policy, Tipton and Krause (2007) propose an effective organisational culture inside the organisation.

According to Da Veiga (2016), this organisational culture advances when management develops a strategy for the organisation. The strategy is often depicted in organisational procedures and policies, and the behaviour of employees becomes evident as they are guided by the strategy of the organisation. Over time, an organisational culture emerges that encapsulates the strategy as well as the experiences employees have when implementing a security culture. Culture plays various important roles within the organisation, for example, all staff need to wear the company's uniform to distinguish one organisation from another. This culture communicates a sense of identity to the members of the organisation. It enhances social system stability by holding the organisation together through the provision of suitable standards on what employees should do or say and it serves as a control mechanism to guide and shape employees' attitude and behaviour. In addition, culture is a combined phenomenon that grows and changes, and it may be designed or influenced by management (Schlienger & Teufel, 2003).

One of the most discussed organisational cultural models widely accepted in the field of information security is Schein's model (Schein, 2009). According to Schein, the greatest danger in understanding culture is trying to oversimplify it. This may be done by perceiving culture as "the way we do things around here" (Schein 2009:21). Another way in which to oversimplify culture is to maintain that it is 'something' that makes one organisation more successful that the other. Schein further states that it is difficult to transform culture since it represents the accrued learning of a group. Culture is learned and shared; it refers to tacit traditions that result in the perception of the organisation or people that this is "the way we do things around here" (Schein 2009:23). The fact that culture is a complex concept is evident in its multifaceted nature, while it is essential that every facet needs to be analysed if it is to be properly understood (Schein, 2009:29). These facets include the following:

- Culture is deep – it is neither possible to change culture easily nor to transform it at will
- Culture is broad – it may be an endless task trying to decipher culture (Schein, 2009)

Culture is regarded as one of the most stable aspects of an organisation.

According to Da Veiga and Martins (2015) it is of high importance that the information security culture of an organisation is constantly improved so that employee behaviour complies with information security policies and regulatory

requirements. The reason for this is that technology can only protect to a point. And because the hackers and bad guys knows this they are targeting the employees of the organisation with different kind of email attacks to get access to the organisations systems. However, if the organisation has trained and security aware employees this task can be made difficult, because employees will no longer be an entry point into the organisation. They further propose that the human aspect be embedded into an information security culture so that instead of employees being a risk to information security they can aid in protecting information (Da Veiga & Martins, 2015).

“Organizations require guidance in establishing an information security-aware or implementing an acceptable information security culture” (Da Veiga & Eloff, 2010:196). According to PWC (2016) a security awareness and training programme is critical to ensure the success of information security policies. It is the role of the organization – a subset of neoinstitutionalism (described below), to ensure adherence to appropriate protocols that adhere to external mandates for compliance. Da Veiga and Martins (2015) explain that an information security culture where training and awareness programmes are provided can positively influence the institution of an information security culture.

The next section provides an overview of information security culture.

2.3 Information security culture

Generally, information security culture can be defined as the values, assumptions, beliefs, attitudes and knowledge used by employees to interact with the organisation’s systems and procedures at any point in time (Da Veiga & Eloff, 2010:12). Malcomson (2009:5) defines security culture as “the values, beliefs, assumptions and attitudes held by the employees of the organisation”. Da Veiga and Eloff (2010:12) concur with Malcomson (2009) that information security is “the values, assumptions, beliefs, attitudes and knowledge that employees use to interact with the organisation’s systems and procedures at any point in time”. Information security is not all about systems; it is also embedded in a culture that perceives, feels, and thinks in the correct way about information security issues (Tipton & Krause, 2007). Information security culture in organisations has been explained using theories adapted from various disciplines such as economics, management, and psychology. This seems to be the conventional trend for an emerging discipline. To this point, perhaps the most popular approach in studying the culture of information security within organisations has been the employment of various organisational culture theories and models. By and large, Schein’s model of

organisational culture dominates this research trend. For example, van Niekerk and von Solms (2010) offer the framework for levels of security culture. This framework provides mechanisms to create and maintain information security culture in an organisational setting.

Lim, Maynard and Ahmad (2009) state that the key challenge of embedding information security culture in organisations is as follows: Information security culture is normally not an integral part of the organisational culture, because security managers frequently have difficulty in obtaining sufficient funding from management to implement information security practices and measures, and then only involve a small group of employees to implement the security strategy of the organisation. On top of this, organisations are typically forced to conform to external audits and regulations rather than the belief of the importance of security practices in protecting organisational information. According to Lim et al. (2009), these findings indicate that further empirical work is needed to determine why organisations still do not take actions to embed information security culture into organisational culture to protect organisational information.

Liginlal, Sim and Khansa (2009) have discovered that mistakes and slips could result in privacy breaches. They state that the management of human error should be a high priority in organisations and propose an error management programme that deals with the root cause analysis of privacy incidents, a periodic evaluation of technical and operational measures, and a defence in-depth strategy to discover the root cause. Padayachee (2012) emphasises the importance of focusing on behavioural issues and building an information security culture when embedding information security in an organisation. A strong information security culture can contribute to minimising the risk of employee behaviour when processing organisation information (Da Veiga & Eloff, 2010). Without a culture of information security, the security procedure and policies will be ineffective in maintaining security in the organisation. In the next section, the researcher discusses how to institutionalise an information security culture.

2.4 Institutionalise an information security culture

Institutionalisation means to produce, build, or give rise to a cause to happen. Thus, creating and information security culture entails the action of producing or building. Various researchers have used different synonyms to refer to the creation of an information security culture, including improving, stimulating, supporting, cultivating, and changing the existing culture to become a more security aware culture (Da Veiga & Eloff, 2010; Schein, 2009). However, before something can be promoted or

cultivated, it must first be established or institutionalised. According to Schlienger and Teufel (2003), it is not possible to establish an information security culture just once and then use it for the rest of the time. On the contrary, it needs to be created, changed or maintained continuously to ensure that it remains consistent with the goals or objectives of the organisation concerned. Ngo, Zhou and Warren (2005) support the institutionalisation of information security culture in an organisation. This entails creating and maintaining the information security culture.

Factors that may add to the institutionalisation of an information security culture include senior management support, security awareness and training, security ownership, an information security policy, incident management, a security budget, and human resources (HR) management and practices (Alnatheer, Chan & Nelson, 2012; ISACA, 2011). Woodhouse (2007) agrees with the notion of embedding information security into organisational culture to guarantee the successful securing of organisational information assets. According to Alfawaz, Nelson and Mohannak (2010), the entrenchment of information security into organisational culture refers to the “information security mode” in terms of which employees adhere to information security policies without being monitored.

Creating information security culture within and organisation brings with it various benefits, listed as follows:

- Standards
- Consistency
- Improved ability to manage risk
- Compliance with laws and regulation
- Improved return on investment
- Trust (ISACA, 2011)

In order to realise these benefits, it is essential that certain challenges are addressed. These challenges include the lack of management support, the information security culture not compromising an important part of the organisational culture, only a small group of people being responsible for implementing information security measures, an inability to obtain the requested budget for security activities, a lack of organisational motivation with regards to implementing security measures, the lack of management support, and information security culture not embedded into organisations.

D'Arcy and Green (2009) show that senior management support is important in promoting compliant and proactive security conscious users. Thus, senior

management must show support through active participation in security activities. Knapp, Marshall, Rainer and Ford (2006) argue that information security is not an integral part of most organisations. There is a problem obtaining sufficient funds from management in implementing information security. Shedden, Ahmad and Ruighaver (2006) discovered that organisations are inclined to treat security spending as a cost and often fight to gain funding for security projects. There also seems to be a lack of motivation to apply security measures after security awareness programmes have been conducted to determine the effectiveness of the programmes. The next section provides an overview of the different methods that can be used to create an information security culture.

2.5 Methods to create an information security culture

Herold (2011) states that creating an information security culture involves instilling security as a way of life as well as integrating security into the behaviour and attitudes of people in respect of a security conscious state. In doing so, organisational culture needs to be considered to ensure that the most suitable controls are recognised and utilised successfully (Da Veiga & Eloff, 2010).

A number of researchers have proposed various methods to create an information security culture within an organisation, including Alnatheer and Nelson (2009), Da Veiga and Eloff (2010), and Gebrasilase and Lessa (2011). According to these authors, the following methods could be used to institutionalise an information security culture within and organisation:

- Organisational culture and ethical methods
- Information security awareness
- Security compliance
- Top management support
- Information security management standardisation and best practices
- Information security policy
- Security training
- Information security risk analysis

In section 2.6, the different processes to institutionalise an information security culture are discussed.

2.6 Process to institutionalise an information security culture

Organisational change is an integral part of life within an organisation because of rapid changes in the external environment. Organisations need to change in order to survive, and therefore the challenge is not whether to change but how to change to

ensure organisational effectiveness. If not managed properly, organisational change may fail. This failure may be attributed to the disregard of organisational culture. Cameron and Quinn (2011) suggest that the culture of an organisation, if managed well, may constitute a competitive advantage and is therefore vital for organisations.

In view of the difficulty involved in changing the values, believes and principles of employees, Schein (2009) proposes an organised change management process to facilitate the creation of an information security culture change in the organisation.

Figure 2.1 depicts an eight-step culture change process as adapted by van Niekerk and von Solms (2006:11). This process includes the following:

- Top management support and commitment
- Defining a specific business problem
- Developing a strategic action plan
- Creating a cultural fit
- Developing and choosing a change leader team
- Creating small wins
- Identifying metrics, measures and milestones
- Reviewing and refining

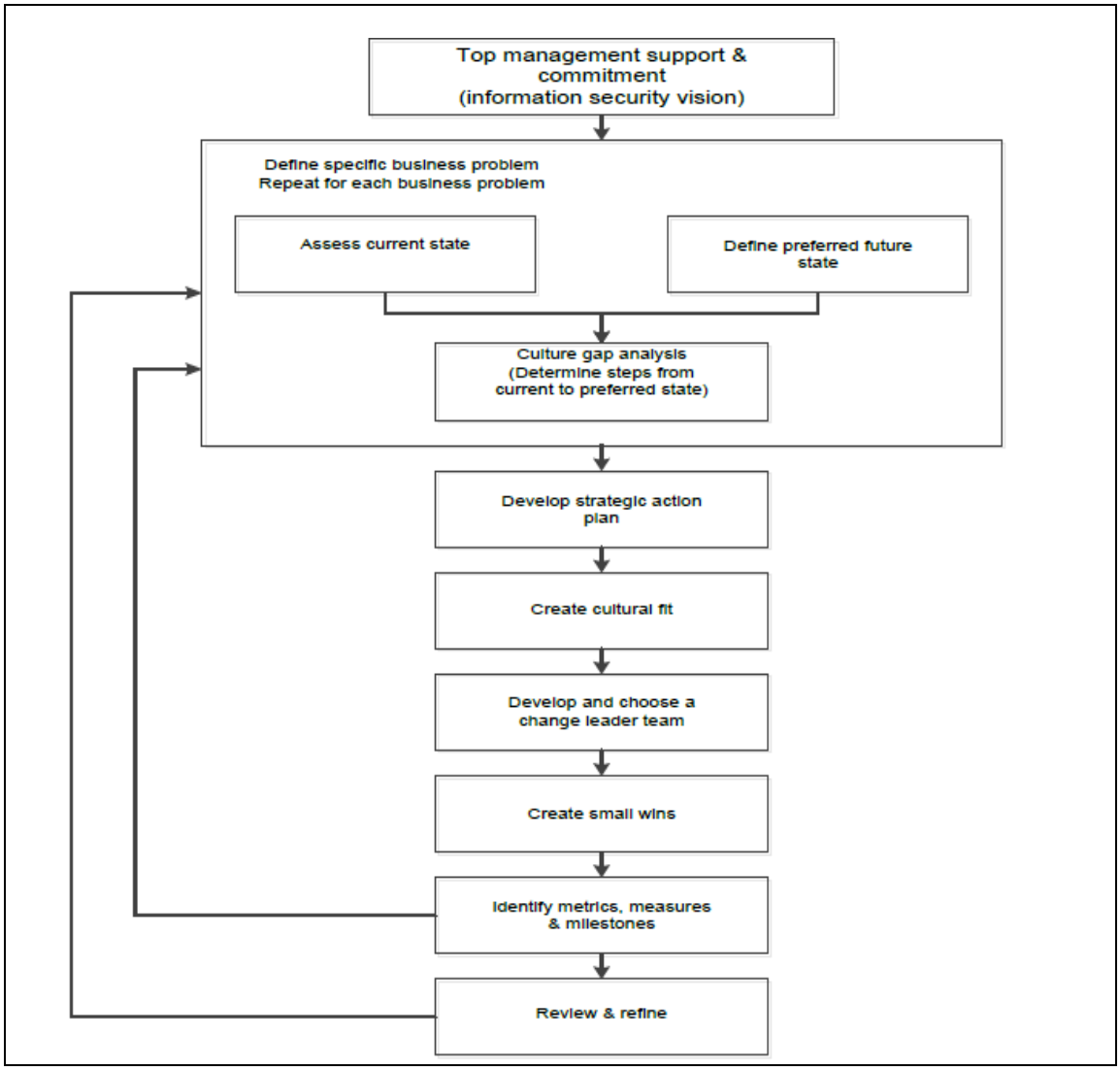

Figure 2.1: A framework for cultural change in organisations
(Van Niekerk & Von Solms, 2006:11)

In the next section, the expectancy-value model is discussed.

2.7 Theory of Planned Behaviour

There exist several expectancy-value models of attitude-behaviour relationship, including the Theory of Reasoned Action (TRA), the Technology Acceptance Model (TAM), and the Theory of Planned Behaviour (TPB), which may be used to explain employees' performance patterns (Huang & Chuang, 2007). The TPB is essential for perceived behavioural control to account for situations where employees lack substantial control over target behaviour (Huang & Chuang, 2007). According to the TPB, individual behaviour can be explained by behavioural intention, which is jointly

affected by attitude, subjective norms, perceived norms, and perceived behavioural control. An employee's behaviour is determined by his or her attitude towards information security. The subjective norms refer to an employee's perception or relevant opinions on whether to perform a particular behaviour that is required. Perceived behaviour refers to an employee's perception of the accessibility of requisite resources or opportunities necessary for behaving in a certain way.

In the next section, organisational cultural theory is discussed.

2.8 Organisational cultural theory

Schein (2009) defines organisational culture as a pattern of basic assumptions, invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration (Schein, 2009). He further defines organisational culture in terms of artefacts, espoused values and shared and tacit assumption (Schein, 2009). The artefacts of the organisation which include the structural settings of the organisation with its technology, office layout, audible behaviours. These are observable, but as an outsider you will only understand how the organisation behaves but you rarely can understand the underlying logic of why it behaves the way it does, and therefore it is hard to analyse an organisational culture only based on this level. On the second level of the organisational culture, there are the cultural values of the organisation. Values are communicated, and employees of an organisation are aware of these, such as company philosophy, norms and justifications. On the third level of the organisational culture, one can find the basic assumptions. These assumptions are lying so deep that the employees cannot imagine what the alternative would be. It can therefore be hard to observe and ask straight questions about these assumptions, since employees might not even understand the question.

Martins and Eloff (2002) use the definition of organisational culture and organisational behaviour to define information security culture (Martins & Eloff, 2002:02). They see it as a set of information security characteristics valued by the organisation, such as confidentiality, integrity and availability of information. Additionally, they also relate it to the assumption about what behaviour is regarded as acceptable in protecting information and what not (Martins & Eloff, 2002:02).

The way cultural theory will be applied to the petroleum organisation, is by looking at the current cultural values that is being used inside of the organisation and how does this influence the current culture of the employees in how they act or behave. If we understand the dynamics of the culture, we will understand the behaviour of the employees in the petroleum organisation. According to the interviews conducted the

interviewer alluded to a behaviour trait of the employees that they feel that information security belongs to the IT department, thus the employees do not feel that their behaviour needs to change when it comes to information security and they can continue to do what they are doing.

In the next section, institutional cultural theory is discussed.

2.9 Institutional cultural theory

According to Dillard et al (2004), institutional theory is concerned primarily with an organisation's interaction with the political and economic institutional environment, the effects of the institutional pressures on the organisation, and the incorporation of these expectations into organisational practice and characteristics. Scott (2008) explains that institutional theory considers the processes by which regulative, normative and cultural cognitive structures are establish for social behaviour. The theory explains how these elements are diffused, adopted, created and adapted over space and time (i.e. institutionalised) and how they fall into decline and disuse.

According to Simone (2009), we often hear about popular culture but less often about institutional culture. An institutional culture can be described as the common values, standards and ideas that permeate the everyday lives of its members, and that are perpetuated by institutional indoctrination, actions and leadership. Simone further argues even though institutional culture is ubiquitous and usually invisible, it is nevertheless important because it has a profound impact on the work environment and the ability of members of the institution to success and prosper.

Similar, Harman (2002:97) refers to institutional culture as historically transmitted patterns of meaning expressed in symbolic form through shared commitment, values and standards of behaviour peculiar to members of the profession, as well as the myths, language traditions, rituals and other forms of expressive symbolism that encompass work.

Thus, if this institutional culture is invisible we as engineers needs to take a different approach to train and educate our employees, instead of using the technology to educate to discover the behaviour and norms of the employees towards IT and what is the reason they are responding in this matter. One of the ways to do this is to have IT security workshops where you introduce the IT security department and what your main goals are as a department. During these workshops make it interactive and ask the employees to ask questions and give feedback how to improve the workshop content. Use this feedback and prepare better for the next workshop with a different department. The value will be must better than sending

information security literature and expecting results from your employees. By doing this you will understand the institutional culture of the petroleum organisation.

In the next section, how to assess an information security culture is discussed.

2.10 Assessment of an information security culture

The researcher can derive from the eight steps of the cultural change process discussed in section 2.6 (Okere, Van Niekerk & Caroll, 2012) that assessment plays a crucial role in the cultural change process. The eight steps are: i) top management support and commitment; ii) define the specific business problem; iii) develop a strategic action plan; iv) create a cultural fit; v) develop and choose a change leader; vi) create small wins; vii) identify metrics, measures and milestones; and viii) feedback and review.

According to Knapp et al. (2006), top management support positively influences security culture. D'Arcy and Green (2009) opine that senior management support in an organisation is important in promoting security. Schein (2009) states that culture change should always be done in a specific business context. Sherwood, Clark and Lynas (2005) agree and state that an information security strategy involves the creation of a strategic plan and vision to address information security risk. Verton (2001) recommends that a change leader is needed because organisations do not change, but people do, and therefore people change organisations. According to Tessem and Skaraas (2005), organisations should measure the level of their in-house information security culture. Puhakainen (2006) believes that giving feedback during security awareness training enhances long-lasting learning results.

The next section examines the role of assessment in cultural change.

2.11 The role of assessment in cultural change

Assessment plays a crucial role in the creation of an information security culture. Culture is an extensive, multifaceted and complex concept that needs to be analysed and assessed at each level in order to be understood (Schein, 2009). The author suggests cultural assessment to solve an organisational problem, enhance efficiency, or realise a new strategic goals. Schein further states that the assessment of culture plays a significant role in the creation of an information security culture (Schein, 2009). In addition, it supports an organisation in knowing its own culture in terms of weaknesses and strengths, and it assists in making strategic choices. Thus, culture assessment allows an organisation to resolve a problem, learn something new, and make changes. However, before this can be done, the

organisation needs to be aware of the way in which the culture may either be a help or a hindrance.

According to O'Donovan (2006), cultural change exists in response to both external and internal forces in the organisation. External forces include political, environmental, economic, and regulatory forces, and internal forces include policies, technology, and rapid staff turnover. These different forces may affect the assessment outcome of the culture.

Cultural assessments also help an organisation to identify both the current and the anticipated state of their information security culture and the areas that require the most attention as well as the improvements needed to achieve the desired information security culture (Ngo et al., 2009). Another reason for an information security culture assessment would be to help an organisation know the behaviour of its employees in respect of information security and to identify key matters, which should be implemented and integrated into the information security culture of the organisation (Gebrasilase & Lessa, 2011). The assessment of the information security culture can also serve as a reminder to management of what the true status of information security is inside the organisation and can thus spur management to take immediate action (ISACA, 2011).Having stressed the importance of assessment in the institutionalisation of an information security culture, it is important to discuss the different approaches that may be used in the assessment of information security culture.

2.12 Current approaches to assess information security culture

Various research studies focus on the assessment of information security culture within an organisation. Table 2.1 presents the research approaches for assessing information security culture as adapted by Okere et al. (2012:49). The first column lists the research approaches in alphabetical order, the second column indicates whether the research approach is focused on the assessment of information security culture, and the third column indicates whether the research approach describes a process for the assessment of information security culture. A tick (√) indicates yes and a cross (X) indicates no.

Table 2.1: Research approaches for the assessment of information security culture
(Okere et al., 2012:49)

	Research approach	Focus on assessment of information security culture	Describe a process for the assessment of information security culture
1	Finch, Furnell and Dowland (2003)	√	X

2	Gebrasilase and Lessa (2011)	√	X
3	Martins and Eloff (2002)	√	√
4	Maynard, Ruighaver and Chia (2002)	√	X
5	Ngo et al. (2009)	√	X
6	Schlienger and Teufel (2003, 2005)	√	√

A high-level overview of each of the above research approaches is indicated below.

- Finch, Furnell and Dowland (2003) assessed information security culture by pointing out the perceptions and security attitudes of end-users and system administrators and ascertaining the differences between the two perspectives
- Gebrasilase and Lessa (2011) used a survey method for the assessment of information security culture in the Hawassa referral hospital
- Martins and Eloff (2002) used an assessment approach comprising an audit process and included and information security culture questionnaire for the assessment of the information security culture within an organisation
- Maynard et al. (2002) developed a research model for information security culture that can be used to assess the quality of an organisation's information security culture
- Ngo et al. (2009) discussed the way in which the level of information security culture in small and medium enterprises in Australia can be assessed
- Schlienger and Teufel (2003) used an information security culture management process that incorporates a combination of methods for the assessment and management of information security culture

2.13 Summary

This chapter explored the topic of information security culture within an organisation. The chapter commenced with background information on the subject of information as a vital organisational asset and the need to protect information to ensure availability, integrity and confidentiality thereof. The management of information security was discussed and the challenges faced by management in achieving the protection of information were stated. Included in these challenges is the 'human factor' concept where employees bypass security controls and thereby cause security breaches.

It is acknowledged that security awareness programmes could succeed in equipping employees with knowledge about security risks. However, these programmes do not

provide any guarantee that employees have mastered the ability to translate the knowledge gained into action, or that the employees will behave responsibly in terms of security in their day-to-day operations at work. This has led to several researchers recommending the creation of an organisational security culture.

Organisational culture was discussed using Schein's model, which is widely accepted in the field of information security (Schein, 2009). The three levels of culture are: i) artefacts, which refer to the visible layer consisting of visible organisational structures and processes that are difficult to interpret; ii) the espoused values, which are not directly visible and which differentiate one organisation from another; and iii) the shared tacit assumptions, which are the ultimate source of values and actions comprising the underlying beliefs and values of the people within the organisation.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

To understand how the research is done, the author explains the terms associated with research methodology. Research methodology refers to the collection of methods, techniques, assumptions and values, and their use in a given research context (Babbie & Mouton, 2001). The most used methodologies in the interpretive research paradigm are the quantitative and qualitative research approaches (Neuman, 2006). The research question, research problem, type of data sources, format of source answers, and the required procedure analysis inform the choice of methodology (Neuman, 2011).

3.2 Research philosophy

Research philosophy can be linked to how knowledge is perceived, meaning the way knowledge is perceived determines how authors will conduct or approach their research (Wilson, 2013). Research philosophy is built on two main pillars, namely the ontology and epistemology approaches. In the next section these two approaches are discussed.

3.2.1 Ontology

Ontology is concerned with the interpretation of the nature of reality (Neuman, 2011). Objectivism and subjectivism are the two concepts that influence an ontological research stance. The main question that gives the ontology insights is whether the existent social entities need a subjective or objective perception. These (subjectivism and objectivism) form the two most central aspects of ontology. According to Saunders et al. (2009:110) subjectivism is about "*social phenomena which is created from the perceptions and consequent actions of those social actors concerned with their existence*." On the other hand, objectivism gives the impression that the existence of social entities is independent and external to the social factors which result in such existence (Saunders et al., 2009). As this research is based on human perceptions and influences in information security, a **subjective ontological stance** has been adopted.

3.2.2 Epistemology

Epistemology is the understanding and knowledge of what the world is about and what truth is developed from its essence (Neuman, 2011). It involves what is needed to produce knowledge about the truth. Epistemology is concerned with the ways we go about acquiring knowledge in the world (Bhattacherjee, 2012). The three epistemological views used in conducting research are interpretivism, positivism,

and critical realism (Wahyuni, 2012). This study follows an interpretivist approach to assist in gaining an in-depth understanding of the research context, including the collection of qualitative data. The epistemology of this research is aimed at exploring how a culture of security can be created inside a petroleum organisation.

3.3 Research approach

When conducting research, there are several approaches or methods that can be followed including mixed methods, a qualitative approach, and a quantitative approach (Mkansi & Acheampong, 2012). According to Saunders, Lewis and Thornhill (2009), the two types of approaches directing the research path to be followed are the inductive and deductive approach. The inductive approach focuses on collecting empirical evidence and building a theory from the findings. The deductive approach is concerned with building a theory with hypotheses and striving to test the validity thereof (Creswell, 2009). Research approach entails the steps made from the broad topical assumptions within a research to the points of collecting, analysing and interpreting data.

3.3.1 Deductive

In deductive reasoning, a theory is used to test a hypothesis. A person can formulate a hypothesis to prove or disprove a theory within the positivist philosophical paradigm. The positivist approach describes (rather than explains) the phenomenon. As a research paradigm, positivism advocates the similarity of, and a need for, a common approach among all scientific disciplines, a model of thinking more pronounced in natural sciences.

3.3.2 Inductive

An inductive approach is subjective in nature and strives to develop a theory from the results of the analysed data (Saunders et al., 2009). Within inductive approaches, a researcher is expected to start the process from a topic which is more specific to his/her topic of interest. The steps of inductive research approach start with observations made by the researcher and proceeds to the theories which are later formulated when approaching the end of the research. The researcher adopted an inductive approach as an investigation was conducted where data were collected from 12 participants to explore how an information security culture can be institutionalised inside the petroleum organisation in the Western Cape.

3.4 Research strategy

Saunders et al. (2009) identifies four main research strategies, namely interviews, case study, survey, and experiment. The research strategy followed in this study is a case study at a petroleum organisation in Cape Town.

3.4.1 Case study

Yin (2003:15) gives the definition of a case study as “an empirical inquiry within its real-life context, especially when limits between the phenomenon and setting are not clearly observed”. According to Yin (2013), the first step is the preparation and determination of the research questions and the second step to case study research, is for the researcher to select various cases and choose on the techniques for gathering data and analysing it (Yin, 2013). A case study strategy is an in-depth analysis of individuals or events, which represents or explains the phenomenon of interest. With a case study strategy, the researcher determines in advance the information to be gathered and the data analysis techniques to be used to answer the main research question. The aim of case study research is to explore the factors that affect a specific situation (Maree, 2007). The case used in this research is a petroleum organisation in Cape Town. The organisation is chosen for its convenience and willingness to participate in the research.

3.4.2 Unit of analysis

According to Babbie and Mouton (2001), the unit of analysis for a case study is rarely isolated from or unaffected by factors in the context in which it is embedded. They emphasise that in order to understand and interpret the case study, a description of the context, in particular, is required. The unit of analysis (UOA) for this research study is the employees who access organisational data, and who, if exposed, could potentially cause a loss of finances or reputation to the organisation. In order to mitigate this risk, the organisation needs to institutionalise an information security culture to make employees aware of their responsibility towards information security. The UOA is the SAP security specialists, compliance analysts, and risk practitioners (see section 4.3 and Table 4.3) employed at the petroleum organisation in Cape Town.

3.5 Data collection process

Generally, there are three ways through which a researcher can collect data while carrying out qualitative research, namely observation, interviews and questionnaires (Wilson, 2013). These methods can be carried out by a variety of ways. Semi-structured interviews are a method for collecting qualitative data for research puposes. According to Wilson (2013) semi-structured interviews are seen as a

hybrid of the structured and unstructured approach where it is based on structured questions but also allows for greater flexibilty for the interviewer and interviewee. Data collection is an organised way of gathering data that answers pre-stated research questions, test hypotheses, and evaluate outcomes. It encompasses both the techniques that can be used and the instruments to be constructed in making the measurements. In order to maintain research integrity, the data collection process should be done accurately using the right methods. In this research, both primary and secondary data sources were used.

The study recognises that a number of data collection methods can be applied. Data collection sources include policies, interviews, direct observation, participant observation as well as examining available physical artefacts (Yin, 2003, 2014). In this research, semi-structured questionnaires by means of interviews were used. An interview guide (Appendix A) directed the interviews. In semi-structured interviews, the respondents plus the interviewer are involved in a formal interview. It is upon the interviewer to develop an interview guide and make use of it.

The following employees were interviewed for this research, SAP security specialists, compliance analysts, and risk practitioners (see section 4.3 and Table 4.3) employed at the petroleum organisation in Cape Town.

3.5.1 Interviews

Interviews enable the interviewer to maintain consistency and be in control of the interview process (Sapsford & Jupp, 1996). The researcher conducted interviews with employees in the petroleum organisation. Permission to contact participants was obtained from the CIO (Appendix B).

3.5.2 Questionnaire

A questionnaire is a sequence of related questions drafted to collect data from the respondents on a subject (Babbie, 2012). The questions can be structured or unstructured. Questionnaires can be used in any type of research, be it qualitative or quantitative, allowing data to be gathered from a large pool of respondents while maintaining control over the responses.

Semi-structured questionnaires are flexible as it can be used to collect data from people in different areas while covering a variety of topics. Semi-structured questionnaires mainly consist of open-ended questions. For this study, a semi-structured questionnaire by means of interviews was used.

3.5.3 Sampling

Sampling refers to any procedure used to select a unit of observation in a research project (Babbie, 2012). Two main techniques, probability and non-probability sampling, can be used in research. Probability sampling is usually aligned with quantitative research and refers to the process where all members of a research population have an equal chance (probability) of being randomly selected to be part of the sample (Neuman, 2011). Non-probability sampling on the other hand is used in cases where the actual location and numbers of a research population are not known and where a random selection process cannot be done. Non-probabilistic sampling includes snowballing, quota sampling, and purposive sampling, among others (Babbie, 2012). For this research, the non-probability and convenience sampling methods were used to select security personnel within the petroleum organisation.

3.6 Data analysis

According to Wilson (2013) analysing qualitative data can be very time consuming and often deals with large amounts of data. The author proposes the following four analytical steps when analysing the data from interviews which can be summarized as i) transcribing the data, ii) reading and generating categories, themes and patterns, iii) interpreting the findings and iv) writing the report. These steps were followed when the data of research were analysed.

Data analysis refers to the drawing of conclusions from raw data (Wahyuni, 2012). All interviews were recorded with the participants' permission and fully transcribed in MSWord format. The transcribed interviews were then given to the participants for validation of the information and correctness of the transcription. Qualitative data can be analysed using a thematic coding approach. This requires reading through all data extensively, summarising all of the data collected, noting all of the similarities that occur in the data, grouping key concepts into themes, and identifying key themes according to their appearances into groups (Thomas, 2003).

As the data were analysed, keywords were identified from the interview extracts and captured on a spreadsheet. Frequently mentioned keywords were grouped together to form a coding scheme according to similarity in meaning and interpretation. Categories were identified according to the number of occurrences and frequency, and relating categories with similar interpretation and representation were further grouped into different themes, either of similar or recurring nature.

3.7 Delineation

The study only focuses on creating a security culture inside a petroleum organisation in the Western Cape. Sources of data are limited to the petroleum organisation. Only security staff were interviewed.

3.8 Ethics

Resnik (2015) defines ethics as the “norms of conduct that distinguish between unacceptable and acceptable behaviour”. Ethical norms can be adopted or learned at school, in a social environment, or in a church during childhood and as people mature. Ethical principles include plagiarism, honesty, informed consent, and permission to publish Myers (2013). Resnik (2015) posits that when people think of ethics, they immediately think in terms of right and wrong. Bengtsson (2016) states that before, during, and after the research process, ethics always has to be taken into consideration. It is suggested that all participants involved in the study should be informed of what the study is about, and they must be ensured that all information collected during the interview processes will be treated as confidential. The participants must also know their right to withdraw their data at any time. Many attempts have been made to determine the effectiveness of ethics (Obalola & Adelopo, 2012), as ethical norms ensure accountability to the public (Resnik, 2015).

Resnik (2015) identifies the following ethical principles:

a) **Honesty**: The researchers must report all their findings honestly and not fabricate or falsify data.
b) **Integrity**: Adhere to all promises and agreements made, also to interviewees or participants.
c) **Openness**: The researchers should be open to any criticism or ideas that may arise.
d) **Confidentiality**: The researchers should protect confidential data at all times.
e) **Animal care**: If animals are used in the research, they must be protected and cared for.

Ethical clearance to conduct the study was obtained from the Ethics Committee of CPUT. Permission to conduct the study was obtained from the Chief Information Officer (CIO) of the petroleum organisation. Both verbal and written (Appendix C) consent were obtained prior to the study. The purpose of the study was explained and the expected roles of the participants clarified prior to commencement of the research. To comply with internationally accepted ethical standards, no names of individuals were recorded on the research instrument. No individual was linked to a

particular completed research instrument, which ensured anonymity. No compensation was paid to any respondent for participation in the study. No respondent or participants were harmed physically, emotionally or otherwise. As with other studies, quality assurance was done with respect to the following:

- Correctness and completeness of open-ended questions
- All participants understanding the nature and consequences of their participation in the study
- The quality of data capturing done by encoders
- Placing all results in the public domain as soon as it becomes available

3.9 Summary

Methodology focuses on how research is conducted, how to find out about things/phenomena, and how knowledge is gained or the different ways of collecting data. In Chapter 3, the author discussed the research methodology followed throughout the research process, which included the research philosophy, research approach, research strategy, data collection techniques, and how the data were analysed.

A subjectivist ontological stance and interpretivist epistemological approach have been adopted. The approach followed is inductive, with a case study strategy. The unit of analysis is the security employees who were non-randomly and conveniently selected. The data were collected by means of interviews, using an interview guide and semi-structured interviews. A thematic analytical approach was followed. All ethical considerations as prescribe by the policy and procedures of the Cape Peninsula University of Technology were followed.

4. CHAPTER 4: RESULTS AND FINDINGS

4.1 Introduction

In this chapter, information of the case used in the research study is discussed. The chapter analyses the interviews conducted during the research process and the findings formulated based on the analysis of the 12 participants' answers. For the convenience of the reader the problem statement, key research questions, and aim of the study are stated below.

Problem statement: The failure to institutionalise an information security culture inside an organisation will cause the continued occurrence of security breaches, costing the organisation reputational as well as financial losses.

Table 4.1: Research questions, methods and objectives

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?			
RSQs	**Question**	**Method**	**Objective**
RSQ 1.1	What are the challenges the organisation is facing when implementing an information security culture?	Semi-structured interviews	To identify the challenges the support personnel are experiencing
RSQ 1.2	What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?	Semi-structured interviews	To identify the employees' reaction towards security changes
RSQ 1.3	What processes can be created inside the organisation to institutionalise a culture of security?	Semi-structured interviews	To identify new processes

Aim of the study: To explore how an information security culture can be institutionalised inside the petroleum organisation in the Western Cape.

In the next sections, the case as well as the findings of the research is discussed. The chapter ends with a summary of the findings and the themes developed from the findings.

4.2 Case study

With the headquarters in Cape Town, South Africa, Engen has a presence in over 20 countries in sub-Saharan Africa and the Indian Ocean Islands and maintains market leadership in its country of origin, South Africa. Engen also exports their product to over 30 other countries. They operate a refinery in Durban, South Africa, which has a nameplate capacity of 135 000 barrels per day, as well as an advanced Lubricant Oil Blending Plant that produces 40 tons of product per hour, totalling

320 000 litres per day on a single shift. Engen has an extensive distribution infrastructure across the region, including depots, terminals, lubricants warehouses, chemical distribution centres, aviation facilities, and a bitumen plant. In addition, the company holds part ownership of 40 000 and 17 000 metric tonne product tankers. Key imports are also secured to supplement demand across their entire network. They also operate an extensive transport fleet of bulk fuel vehicles, with a staff compliment of 4000 employees using Microsoft and Linux servers.

4.3 Participant description

To be able to answer the research questions, 12 interviews were conducted at Engen's headquarters in Cape Town. All interviews were done face-to-face and recorded on a cell phone, and the recordings were transcribed using the Microsoft Office Word application. The interviews were scheduled in the available meeting rooms (Table 4.2) at the head office building in Cape Town. All participants agreed to participate in the research and signed the CIO consent letter (Appendix A). The interview location is situated in the central business division of Cape Town (Figure 4.1).

An interview guide in the form of open-ended questions was used and interviews took approximately ten (10) to thirty-five (35) minutes to complete. Some participants answered the questions much faster and had a little to say, whereas other participants took longer to answer the same questions; thus according to the recordings, this was the time indicated.

Table 4.2: Interviews per department

Participant	Location of interview	Interview duration	Date of interview
P1	Meeting Room 4050	14 minutes	01/11/2017
P2	Meeting Room 4054	20 minutes	26/10/2017
P3	Meeting Room 4050	17 minutes	31/10/2017
P4	Meeting Room 4050	24 minutes	01/11/2017
P5	Meeting Room 4050	16 minutes	30/10/2017
P6	Meeting Room 4050	24 minutes	31/10/2017
P7	Meeting Room 4050	12 minutes	03/11/2017
P8	Manager's Office	12 minutes	02/11/2017
P9	Meeting Room 4050	11 minutes	27/10/2017
P10	Meeting Room 4050	13 minutes	26/10/2017
P11	Meeting Room 4050	31 minutes	02/11/2017
P12	Meeting Room 4050	35 minutes	03/11/2017

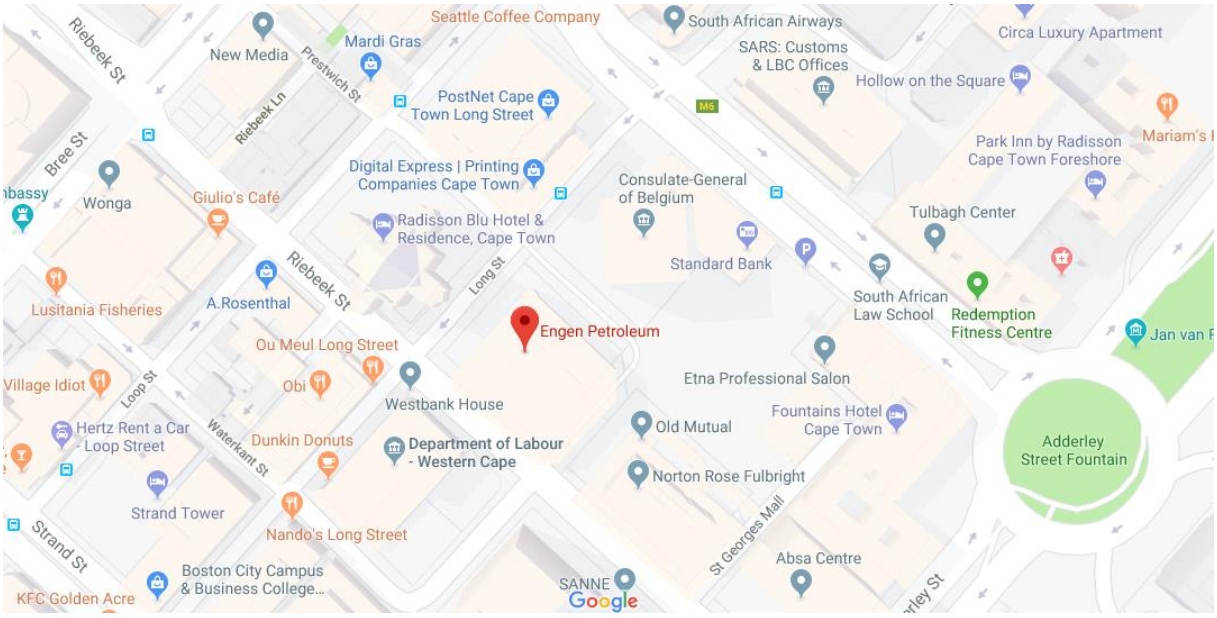

Figure 4.1: Engen Petroleum offices where the interviews were conducted

All participants work in the IT Security and Risk team at Engen Petroleum Limited. The department is sub-divided into different sections: IT Security, SAP Security, Risk team, and IT compliance. From the twelve (12) participants, nine (9) employees are permanent and three (3) are contractors. Their years of service range from six (6) months to thirty-five (35) years.

Table 4.3: Summary of all the participants' information

Code	Job title	Permanent/Contractor	Years in service
P1	Security Specialist	Permanent	17
P2	Compliance Analyst	Permanent	2
P3	Security Specialist	Permanent	5
P4	Security Analyst	Permanent	35
P5	Security Specialist	Contractor	1
P6	Senior Security Specialist	Permanent	9
P7	Junior Security Specialist	Contractor	1
P8	Manager Information Security & Risk Management	Permanent	15
P9	Junior Security Specialist	Permanent	5
P10	Security Specialist	Contractor	6 months
P11	Principal Security Specialist	Permanent	15
I12	Process Practitioner: IT Risk	Permanent	3

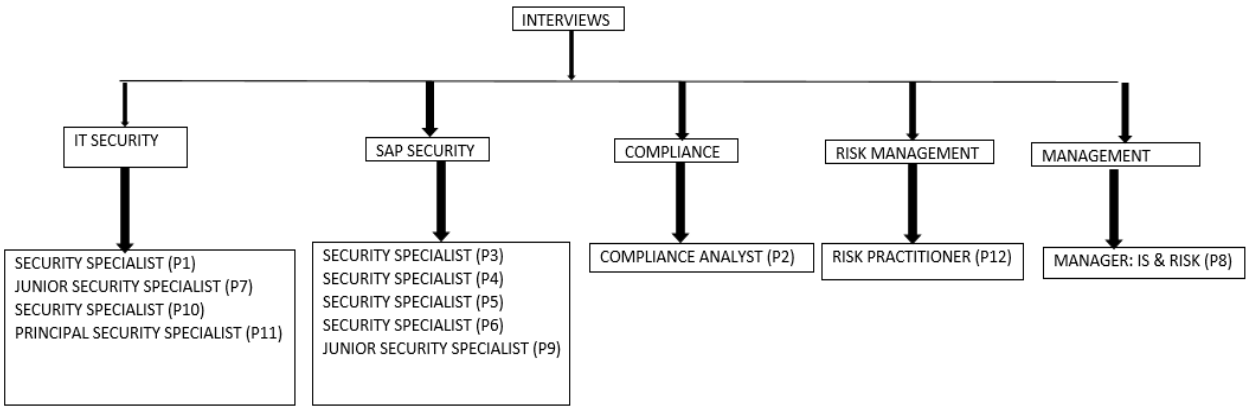

Figure 4.2: Interviews per department

Participant 1 (P1) is an IT Security Specialist at Engen Petroleum Limited. He is responsible for the operational IT security activities in the IT Security department. Although he has seventeen (17) years of service at the organisation, he has only been working for the last two (2) years in the IT Security department. He worked with the Technical Support team as a Senior Technical Specialist as well as End User Support Specialist during his 17-year career at the organisation.

Participant 2 (P2) is a Compliance Analyst at Engen Petroleum Limited and is currently a year in this position. Before this, he held the position of Junior Technical Specialist in the Technical Support team. He is responsible for all the compliance duties inside the IT department.

Participant 3 (P3) is a SAP Security Specialist at Engen Petroleum Limited. She is responsible for the SAP operational security activities in the department. She has been a contractor for three (3) years before she was made permanent two (2) years ago.

Participant 4 (P4) is a SAP Security Analyst at Engen Petroleum Limited. He is responsible for the SAP operational security activities in the department. He has 35 years of service at the organisation.

Participant 5 (P5) is a Security Specialist at Engen Petroleum Limited. He is responsible for the SAP operational security activities in the department. As a contractor, he has two (2) years of service at the organisation.

Participant 6 (P6) is a Senior Security Specialist at Engen Petroleum Limited. He is the current team leader and responsible for the SAP operational security activities in the department. The SAP Security Specialists and Analysts report to him.

Participant 7 (P7) is a Junior Security Specialist at Engen Petroleum Limited. She is responsible for the IT operational security activities in the department. As a contractor, she has a year's service at the organisation.

Participant 8 (P8) is the Manager of IT Security and Risk Management at Engen Petroleum Limited. As the Manager of the department, all the participants who took part in this research study report to him. Although he has fifteen (15) years of service at the organisation, he has only been manager of this team for the past five (5) years.

Participant 9 (P9) is a Junior SAP Security Analyst at Engen Petroleum Limited. He is responsible for the SAP operational security activities in the department.

Participant 10 (P10) is an IT Security Specialist at Engen Petroleum Limited. He is responsible for the IT operational security activities in the department. As a contractor, he has six (6) months of service at the organisation.

Participant 11 (P11) is a Principal Security Specialist at Engen Petroleum Limited and the current team leader of all the IT Security Specialists, including the Junior Security Specialist. He is responsible for the operational security activities in the department. He has been the Security Architect before he was transferred to the security team.

Participant 12 (P12) is an IT Risk Practitioner at Engen Petroleum Limited. He is responsible for the IT risk activities in the organisation.

Table 4.4: Participant details

Participant	Job title	Years of experience	Work specifications
P1	Security Specialist	17 years	Responsible for the operational IT security activities in the department. Although he has seventeen (17) years of service at the organisation, he has only been working for two (2) years in the IT Security department. He has worked with the Technical Support team as a Senior Technical Specialist as well as End User Support Specialist during his 17 years career at the organisation.
P2	Compliance Analyst	2 years	He is responsible for all the compliance duties inside the IT department.
P3	SAP Security Specialist	5 years	She is responsible for the SAP operational security activities in the department. She has been a contractor for three (3) years before she was made permanent two (2) years ago.

Participant	Job title	Years of experience	Work specifications
P4	SAP Security Analyst	35 years	He is responsible for the SAP operational security activities in the department. He has 35 years of service at the organisation.
P5	SAP Security Specialist	2 years	He is responsible for the SAP operational security activities in the department. As a contractor, he has two (2) years of service at the organisation.
P6	Senior SAP Security Specialist	9 years	He is the current team leader and responsible for the SAP operational security activities in the department and the rest of the SAP Security Specialists and Analysts report to him.
P7	Junior Security Specialist	1 year	She is responsible for the IT operational security activities in the department. As a contractor, she has one year of service at the organisation.
P8	Manager: IT Security & Risk Management	15 years	He is the Manager of the department and all the participants who took part in this research report to him. Although he has fifteen (15) years of service at the organisation, he has only been manager of this team for the past five (5) years.
P9	Junior SAP Security Analyst	5 year	He is responsible for the SAP operational security activities in the department.
P10	Security Specialist	6 months	He is responsible for the IT operational security activities in the department. As a contractor, he has six (6) months of service at the organisation.
P11	Principal Security Specialist	15 years	He is responsible for the operational security activities in the department. He has been the Security Architect before he was transferred to the security team.
P12	IT Risk Practitioner	3 years	He is responsible for the IT risk activities in the organisation.

4.4 Findings

As stated in Chapter 3, interviews were transcribed, coded (keywords and key phrases), and summarised; categories were developed and findings were drawn. From the findings, themes for discussion were identified. The interview appointments were set up via Microsoft Outlook, which then led to the actual interviews.

In this section, the interview responses collected during the research process are discussed. Based on the answers of the 12 participants, findings are drawn for each interview question. The section is presented in such a way that the research question (RQ), research sub-questions (RSQs), and interview questions (IQs) are linked.

4.4.1 Interviews

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ .1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

According to participants (P) P4, P5, P8 and P9, users do not adhere to the requirements set out by the IT Security department; they feel users do not have the necessary knowledge of IT security. Although the necessary security awareness information is being distributed via email communication and posters, users still do not adhere to the requirements. The participants suggested that the department looks at other methods of security education. P8 said:

> "I don't think so. I think... the Engen employees are not educated enough with regards to security; first to what the function is and what it tries to protect us against, and what the risk currently exposes in the environment. So more work needs to be done in that regard because that will build culture in the organisation, and that can be done through various communications, training, etc." (Appendix B8, IQ 1.1.1).

However, P7 disagrees. P7 stated that some users are educated already, because they adhere to the requirements set out by the department: "I will say yes and no. When I say yes, you do get those that… they do adhere based on… they do follow whatever they [are] being told, for instance they do read the posters when it is put out there" (Appendix B7, IQ 1.1.1).

P11 said users are educated enough because security awareness communications are being shared with them; however, before the users adhere to the security requirements of the department they need to have a full understanding of what the requirements are all about and what the risks involved are if they do not adhere to it. P11 elaborated:

> "I think where we find issues of users not adhering to requirements, I like to think that the most part is because they are not aware of the requirements, and if I can liberate [sic] a bit more on that, that really comes down to building a resilient organisation. It comes down to users' awareness of risk and how responsible they are towards that risk, and I think if they have a better understanding of what that risk is and what the responsibility towards it [is], then I think it would make a better, It would make adhering to those requirements for the users a bit easier" (Appendix B11, IQ 1.1.1).

P10 is in support of P11's explanation and stated that once users understand the consequences of what can happen to the organisation they will make an effort to adhere to the requirements if the network is breached:

> "I would say it's a bit of both. Some users actually adhere but [in] the most cases you have to consciously make a follow up because most of the guys fail to understand the after effects of these breaches or when things go south. I guess the old gap is us as… or me coming from [an] information security background, we tend to be too technical. It's mostly like technical theory not really sure or put across show them like in real life scenarios why this should not be done" (Appendix B10, IQ 1.1.1).

Finding 1: Users do not have the necessary knowledge of IT security and need to be educated on this topic

Finding 2: It is not clear what risks the department is protecting the organisation against

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

P1, P3, P6, P8 and P9 mentioned that users do not know what their responsibility is towards information security because the organisation has the necessary security controls in place. P1 explained that if the users have an opportunity to bypass the controls, they will not hesitate to do so: "The role that they have to play do I believe it. I don't think so and I don't think so because I think that if they could bypass the controls that's [sic] been put in place they would bypass it. So I don't think they will adhere to it" (Appendix B1, IQ 1.1.2).

P3 said that users do not take the necessary responsibility when it comes to information security and they want to be spoon-fed by the IT staff:

> "No, I do not think so. I think basically from a business perspective, they don't see the IT part of it because in their eyes it's our responsibility, so it's like this division that's drawn. That's your responsibility and we're business so I think a lot of you know and like to be spoon fed and a lot of it is they don' take that much responsibility" (Appendix B3, IQ 1.1.2).

P6 is in support of P3's explanation and stated that users do not understand their responsibility and think that a security breach will never happen to them: "I do not think they understand the full responsibility although I think they are aware of what the implications are, but I think they have 'this will not happen to us' attitude" (Appendix B6, IQ 1.1.2).

According to P2, P4, P5, P7 and P11, users do know what their responsibility is because major security breaches such as the *Wanna Cry* and *Petya* outbreak made it on the local news on the local television station. P2 said: “Yes, because it is out there; we hear about cybercrimes because IS security or cyber security been made aware of the *Wanna cry* outburst”. Recently the Liberty insurance company was breached and it all was on the television station, internet websites and local papers. This is another example where an insurance company was breach through a phishing email attack. The good thing about this hack is that all clients of this specific insurance company was notified via SMS. If our employees are a customer of Liberty they received this message, and although something bad happened this can be used to inform the employees what we are trying to do. (Appendix B2, IQ 1.1.2).

P4 agrees with P2. P4 stated that he feels the organisation is sending regular security awareness communication to all the users in the organisation. Some of the users do read the security awareness communication; however, they are not forced to read these notifications. Some users even delete the notification emails without reading it. If there is a way to force users to open and acknowledge reading the email instead of simply bypassing the actual notification, it will make them more aware.

Finding 3: Users do not know what their responsibilities are towards information security

Finding 4: Security communication is not recognised and understood

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

The majority (8) of the participants (P1, P2, P3, P5, P6, P8, P9 and P12) feel that users are not aware of the risk of not following information security procedures. P5 explained that users are still sharing SAP passwords among each other, and this is why he feels they do not understanding the risk of their actions: “Not fully. They may be aware but not really worried about it, for example, the sharing of log on details, only that happens so often and it’s a risk. I mean it can get into the wrong hands” (Appendix B5, IQ 1.1.3).

P6 elaborated by saying that users are not accountable because there is no repercussion when they do not comply with the information security policy: “I don’t think we have ever made an example of anybody, so I don’t think they are aware.

We don’t have a culture of holding people to Engen's standards or Engen's policies” (Appendix B6, IQ 1.1.3). P8 stated that the reason why users are not aware of the risk is because they do not understand the concept of IT security and risk management. In the past everything has always been open, for example inserting memory sticks into computers, and they cannot comprehend why it is now being blocked by IT: “No, I do not think so. I do not think they understand the concept, the lack of concept, they do not understand the risk exposed to it and how the companies are exposed when they are being breached” (Appendix B8, IQ 1.1.3).

P7 indicated that although the organisation has the necessary controls in place, users will always be curious and this is causing them to open phishing emails:

> “That could be debatable. Some are aware some are not, they just found a reason not the obey, for instance, some of them I think, for an example, I think them some of them [are] more open for curiosity situation where they want to see, if I do this what’s, going to happen, not knowing the consequences of what would happen if they do that” (Appendix B7, IQ 1.1.3).

P11 also mentioned that because users are not working in the IT department, they are not aware and not even worried about the risk they are causing when not following the security policies. P11 said:

> “I'll say for the most part we have some users which, who are aware, and [the] majority who are aware will probably be an IS. I think the further you move outside of the IS, I have a feeling that they are not aware of [the] system... so they [are] not aware that if they... as an example, they plug in a USB stick which has a piece of malware on, they are not aware of the impact that malware can have” (Appendix B11, IQ 1.1.3).

Finding 5: Users are not aware of the risk of sharing passwords among one another

Finding 6: Users are not accountable for security breaches, as there is no repercussion when they do something wrong

Finding 7: Users do not fully understand the different ways hackers are attempting to breach the company’s network

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

The majority of the participants replied that users are not taking the necessary ownership they need to. P2 said that users are forgetting their responsibility when it

comes to the security of using of a computer and because the organisation has an IT department, they are passing that control over to them:

> "No, this is purely because I'm speaking from a human point of view. Humans tend to pass the buck or not take responsibility if something goes wrong, they then in retrospect, they tend to want glory or fame when things go right. So I don't think they want to take responsibility for it but somebody needs to answer at the end of the day. Although the CIO makes the decisions the users should take responsibility for any breaches" (Appendix B2, IQ 1.1.4).

P10 mentioned that users will just shift the blame to IT: "No, users, from my experience and my own opinion, users tend to play the blame game; they always blame it on the IT department or the Security department that, if this was in place... so it is always people pointing fingers to departments in charge" (Appendix B10, IQ 1.1.4).

P11 argued that information technology is very complex and users struggle when they need to manage the information of the company – what needs to be allowed or not, what needs to be treated as confidential, or even taking home confidential company information on a memory stick:

> "I have seen where users are very aware of their actions and they act responsibly. I don't think users act irresponsibly and I have mentioned before, I think it definitely comes back to, it's all about information. So even if we take a look outside of security the big battle that IT has always had is to get the users or the owners of the information to be accountable for the information and that they should, and to making sure who has access to it but also make sure that it is used in a diligent way. That is a challenge. I see this challenge even today with IT and the owners of the information taking accountability for it, so we can then extend that to the security aspect" (Appendix B11, IQ 1.1.4).

According to P12, users need to be held accountable when handling company information during and outside office hours:

> "No, I think ownership especially you need to take the example of generic accounts, you can't pinpoint who's doing what and so forth. I think especially in that, and I know that, maybe a bit more exceptional, but I think in those instances people sometimes do what they want to do and they kind of like when pinpointing comes back, it's difficult to know who it was in the first place from and accountability prospective. So I personally don't think so" (Appendix B12, IQ 1.1.4).

Finding 8: Users do not take ownership; they leave the decision to the IT department

Finding 9: Users need to take responsibility and should not pass the blame to IT only

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

P3, P4, P6, P7, P9 and P11 mentioned that user education is greatest challenge in instituting an information security culture in the organisation. Although security awareness communication is distributed via posters and emails, P3 said that all new employees should receive this training during the induction process when new employees join the organisation:

> "I think like, you know our world [has] a bit more of a complicated side, but like a very low level maybe integrated with the on boarding, the induction. You know, just have somebody from security start speaking to them, they actually start getting comfortable with the idea of security and you know, like it's there to...not a business us and them.." (Appendix B3, IQ 1.1.5).

P6 said that there are not enough staff in the IT Security team to focus on security education, thus not enough time is given to this activity. He also mentioned that previously when he worked on a project in the organisation, a Project Officer was appointed to ensure appropriate email communication to the users for each meeting, and that this contributed to the project's success and necessary buy-in from the users throughout the project. P6 said:

> "I do not think they really have the workforce to have somebody that sends documentation or even a one-liner once a week or once a month. We have the facilities to use and to share information, and I don't think that we phantom that into our tasks, and besides, I don't know how people will read it. That's why I say you can't go through a whole article once a week, just a one-liner. Well, I can understand that the people want their emails to be sent" (Appendix B6, IQ 1.1.5).

P2 mentioned that there are too many silos in the organisation and between departments that can cause a problem when instituting and security culture:

> "The biggest challenges, as I have mentioned before, is [sic] of the silos that is [sic] here. The people protect the environment tremendously. They do not want our departments to scratch out their environment or they are very protective of their environment. Something else I've noticed also is processes – this company is very process-driven and sometimes these processes have an impact on the actual work that needs to be done because processes take time. Because approvals needs [sic] to be done, it goes through a whole long list of approvals, goes to a whole list of testing, a whole list of everything before the actual work gets done. So processes need to be re-looked at this

company through maybe streamline it and make it more effective. For now, that's the only thing" (Appendix B2, IQ 1.1.5).

P12 supports the view of P2. P12 stated that because of the silos that exist, users are resisting any new changes that are being introduced in the organisation:

"Definitely resistance to change. I think people especially at Engen, some of them have been in there jobs for 20, 30 years and I'm not only referring to them because there's people that's been here for 2, or 3 years also, but I think historically our organisation has done things a certain way now and I have personal experience of this where you come in and try to implement new measures or sharing information to improve things and you kind of detour a big wall, because firstly, there is no buying in from top management. When I say top management, I'm talking senior management, which is below your CIOs. The CIO may be on-board but below CIO, so I think if your senior managers are not on-board with the importance of security, it's very difficult to go forth and actually implement what you need to implement" (Appendix B12, IQ 1.1.5).

Finding 10: There are no security policies and procedure training for new employees

Finding 11: Too many silos in departments is part of the problem why it is so difficult for users to change

Finding 12: Some older employees are not open to new ideas and resist any new changes

Finding 13: There are too many processes inside the organisation

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

The majority (9) of the participants, P1, P2, P3, P5, P7, P9, P10, P11 and P12, mentioned that the IT Security department provides adequate security training during security changes in the organisation. Current security training is in the form of posters and email notifications.

According to P9, the training is sufficient and the department needs to verify the users' understanding of the message conveyed to them. For example, when an email is sent out, the department has no compliance measure in place to determine

who is reading the email or who is simply deleting the actual email, but most of all, do they have an understanding what the department is trying to say: “I will say they try but the problem is the users understand that’s the challenge... they try to communicate but also they don't follow up... the users” (Appendix B9, IQ 1.2.1). P11 supports P9 and feels that additional follow-up training is needed:

> “I think any training needs to have a measurement of compliance, so we can’t just deliver training and expecting the user base to consume it and be under the impression or expectation that we have successfully delivered training. So we definitely have to follow up that training with compliance checking, so we provide a number of, we provide various training methods by using common organisational methods which include internet, email we are now using... which is a third party service, especially for phishing attacks. We [are] providing that service as a level of training to it as well. If we do not take compliance checking then it’s very difficult for us to actually gauge how we improve on our, how we actually do it. So is our training working? Is it not working? And I think with our tech compliance checking it’s going to be very difficult to gauge the level of awareness” (Appendix B11, IQ 1.2.1).

P12 explained that not enough is being done in terms of setting security measures:

> “I don't think they are providing adequate training now. I think they maybe do provide a level awareness through communications but I don't think they provide adequate training around security measures and so on, even bringing in new policies around on how you must do things and maybe if you got mobile devices you need to put security settings or whatever on there. I think we should be having things like training on mobile devices, for example, we are able to access our Engen emails on our mobile devices right through the Internet and webmail now you download an attachment from the email onto your phone, your personal device that does not always have security measures in place – doesn’t actually know how to deal with that. My answer would be no, they don't know how to deal with it” (Appendix B12, IQ 1.2.1).

Finding 14: No security communication compliance records are kept

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

P1, P3, P4, P5, P6, P7, P9, P10 and P12 mentioned that email notification is used the most. Security posters displayed on notice boards as part of the security awareness message support this. P4 said that the IT Security department could use other methods as well to spread the message of awareness, for example distributing flyers on the desks of users.

P11 mentioned that more face-to-face communication is needed than sending emails. Another method to verify compliance is running phishing assessments and targeting the users who are still opening the phishing emails. P11 said:

> "I touch[ed] on the mechanism in the previous question briefly, so the mechanism are [sic], we do face-to-face, we do pending email, internet. We have [a] third party service that has built-in training with it and those services are Mimecast, email hygiene service. There is [sic] phishing assessments; those have built training with it. We have, those are predominantly the user facing training that we do…" (Appendix B11, IQ 1.2.2).

Finding 15: A different communication strategy than what is currently being used inside the organisation is needed

Finding 16: No or little assessments are done after security messages have been delivered

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

P2, P3, P4, P5, P6, P7, P8, P9 and P10 mentioned that action should be taken against the users who do not comply with the information security policy. P2 said that the organisation should make information security part of their key performance indicators (KPIs), because only then employees will understand the importance of what the IT department is doing:

> "It should be put in your KPI, how many times you breach a certain incident, or a security incident should be put in to reach a certain amount, whatever the case. Maybe then you score a zero or you will score a 3 or 2 of 5 or whatever the case may be because this should be part of your KPI. I believe that people should adhere to it and there should be some punishment attached" (Appendix B2, IQ 1.2.3).

P4 stated that in the past, managers of users who did not comply were informed, but this practice has fallen to the wayside and is not done anymore. P4 said:

> "Well, I know there was some action taken against users that visited inappropriate sites. If it keeps on they would, currently we've got some lock down on that there are ways and means. If you know how to get passed it, then can you pass it? Maybe they should just be more vigilant about the user, not only say, look we give you the companies to judge. We have caught somebody out already where they have applied for a post. In the past we gave you a password, nowadays we send it to you and the self-service password that you can change, your password" (Appendix B4, IQ 1.2.3).

P11 feels users should not be punished as the department needs to check for compliance with security training first; however, a user who has completed the training and then transgresses should be punished. P12 said:

> "There is a big element, before they need to be held and consequence management and all that than if you had done that and you [have] done it substantially and effectively over a period of time, then we go to a point where we say the education is done, now you know what now guys. We will have some level of consequence management for the fact that people are abiding by policies. Some policies are quite straight forward. Annually you stay away from work, I would probably ask most employees, they will be fully aware you need to put in a leave request first. Are people aware of [the] information security policy? Are they aware of all of those things? I think to some degree, but I think to a degree not. And I mean, to have consequences and consequence management, you need to be able to hold them to something and if they can prove that this is communicated to them, then it becomes a legal matter and all of those things. So I think there is a range of stuff, but bottom line is, in future when this thing is more solidified and all of those things, then we can kind off move to" (Appendix B12, IQ 1.2.3).

Finding 17: Users who do not follow the security policies should be punished as part of consequence management

Finding 18: Key performance indicators in terms of information security are not part of the user's job description and appraisal system

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

Most of the participants (P1, P2, P3, P4, P5, P6, P9, P10 and P12) stated that the current security awareness programmes are not effective. P1 said that after a phishing campaign has been conducted in the organisation, users still open phishing emails:

> "Judging by the amount of breaches we had with the testing on the phishing, I don't think its effective for the users to continue although I think that from Engen's side, we are trying to keep people informed, but it does ultimately fall on the user to actually look at the information, the access given, the information they are given, to actually look at the information and understand it. To a respect, the way I see it, that you can only do so much. You can't force somebody to read an email, you can't force somebody. If they do not understand, they probably won't ask. I do believe we do provide adequate, or I think we do provide adequate information. Forcing people to go through security training is a brilliant idea. I think the constant testing on the phishing campaign, I think it's good. We do keep people up to date with the latest trends most of the time. I think it is falling a bit on the wayside. The relevant

topics are given to the people, to actually, I do believe it will provide" (Appendix B1, IQ 1.2.4).

P6 said that while the department is simply doing security awareness communication, there is a need for actual training where users are brought into a room and trained on security:

> "I don't think so. I think in the new structure, I think that we should perhaps engage with the training department and maybe work on a section in the Engen induction where they go through the Engen policies and they should actually brief people on what can be expected if you breach. So that person will know that everybody has been communicated to and it's not like you can say, I didn't know. I think there is a definite place for that in the induction and I think we should engage with the training department to have that included" (Appendix B6, IQ 1.2.4).

P8, the manager in the department, feels that as a department they have done enough with the allocated budget and suggests that more money needs to be made available in order to do even more: "I don't think its ineffective at the moment [be]cause there is [sic] a lot of talks about that we've brought along, like password complexity, but I think the... for more effectiveness around it. Yet again, budget spending, if we had unlimited budgets we could have done a lot of training. I think users would be educated, but it is a question around budget" (Appendix B8, IQ 1.2.4).

Finding 19: There is a lack of training and as a result, users are still clicking and opening phishing emails

Finding 20: There are budget constraints on security training and awareness

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

Some of the participants, including P6, P7 and P9, argued that the department needs to look at a better communication strategy to spread the message. P7 stated that they only target the users in the offices. P6 elaborated that the IT Security department needs to be more visible; IT staff need to walk around the building to check for computers that are not locked and inform the users about the dangers of leaving computers unattended. P6 said:

> "…my earlier example is that when I walk around, I don't go walking around on other floors. So when I walk around, I walk around on our floor where we have people in our own team in security minded people that walk away from their PC's and leave it unlocked. There's people in IT that in my opinion they shouldn't be told about security, that should be part of their work culture and they themselves walk away from their PC's leaving it unattended, open, and unattended, and so it's like living by example. That's [why] we as IT must adhere to Engen's policies" (Appendix B6, IQ 1.3.1).

P12 stated that the department needs senior management buy-in when doing awareness or training:

> "Number one, I think the organisation board from top down, when we did officially phishing exercises, board members, one of the high level board members that was actually in the phishing emails, so they responded to the emails. Basically what I'm saying is, even if you have 30 years' experience or you [are] 5 year[s] old, you can be caught by these things, right. So, number one, [the] board needs to be on board with cyber security. I'm aware that it is a board agenda item, so it is discussed. The question is, what goes forth from right there, right, and are [sic] the mechanism that comes down from the board all the way through the heads of the areas such as the general managers, are they effective and do they understand all of those things? Personally, I don't think that our general managers are fully clued up on information security and what they need to do in their areas in relation to information security, and I understand that because they have a business to run, we have not actually done a lot of training directly with them, maybe come to them... So basically, top down, I know the CIO is actually presenting at the board, so they are generally aware, but the question is, how are they aware in relation to the organisation? So when you keep buying from the top management, which is the board, then you get the GM buying, then you get the elderly level buying, which is your senior managers, then all the way from there go through because when I have conversation with people in… level in the business they are financing perks and all of these things, but when it comes to managing even service providers from a security prospective they have absolutely no knowledge" (Appendix B12, IQ 1.3.1).

Finding 21: There is a lack of management buy-in when it comes to security

IQ 1.3.2: *How would you describe the information security culture at Engen?*

According to P2 and P3, there is hardly any culture when it comes to information security, and all the users want access without proper justification. P3 stated: "I don't think we have too much of a security culture, [be]cause everybody, especially where access is concern, they just want access. They don't think there is [sic] consequences to what they are asking and it start[s] with management coming down

on you to get that... not listening to people problems... We basically try to explain it at first and if they still don't, we escalate it on our side" (Appendix B3, IQ 1.3.2).

P8 said he feels improvements have been made in the organisation, because employees and management are starting to talk about security:

> "I think in the last 2 years it has improved [be]cause I see a lot of people talking about ballpark security. More people have conversation concerning hector hackers, etc. I think there is a greater understanding around and the term hacker has been commercialised. A lot of people have now taken on what is a hack, but obviously the technical behind it understand[s] the concept of hacks. I think it has improved, but I think there is more room for improvement. I would say there is some understanding around what security means to Engen" (Appendix B8, IQ 1.3.2).

P9 believes the reason why it is so difficult to institute a culture of security is because users are of the opinion that information security belongs only to IT staff: "I... everyone is doing what they are doing... If you are not in security, you are not worried about this thing, the system, because, and also the security people…" (Appendix B9, IQ 1.3.2).

P11 mentioned that there is some form of culture in the organisation; however, some processes need to be looked at and management needs to make more funding available for information security. P11 said:

> "There seems to be a certain level of culture that prevails in the oil and gas industry. In large areas of the business there is really risk. They work in refining processes, they work with refineries, and you know, if something goes wrong it has an impact, not only on the financial reputation, it also has an impact on life. And so I think that's where the risk comes in, and people like to be very aware of the risk. I think what is happening now is quite clear. Over the last few years the culture of information security has been one of a lack of awareness. They haven't been aware of it and only now we see the threats globally that are impacting infrastructure, like energy, like oil and gas, or include oil and gas, which is now bringing information security up into the board level. Now that its reach the board level, its actually started to have a wider impact against all stakeholders within the organisation which puts the ones at risk, some risk, or put ones on the individuals to be savvy when it comes to information security, saying that I think the users and the employees and all in the gas environment still need a lot of help and understanding to what information security is or what cyber security is…" (Appendix B11, IQ 1.3.2).

Finding 22: The user's perception of what the Information Security department is doing needs to change

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

Fifty percent (50%) of the participants (P1, P3, P4, P5, P8, P9, P10 and P12) are of the opinion that although some form of security awareness is being done to communicate the message to the users, a strategy other than email communication and posters needs to be looked at to deliver a more effective message. P1 said the organisation needs to look at introducing security awareness videos or information cards: “I think to get the people talking, and an example I would say is well, [it] once again comes back to the posters. I think maybe we should use [a] video, [a] very short video. I think maybe little information cards, small little ones, that just in your face information” (Appendix B1, IQ 1.3.3). P8 is of the opinion that the organisation needs to go back to the induction programme of new employees and introduce the security programme at this event.

P12 agrees with the change of format of the security awareness material, and security educational videos should be used to educate the users:

> “…better funded initiatives around security awareness to the degree where I mean, I know, when the one organisation did the exercise they actually ended up getting into the building via the fact that they had a familiar face and they end[ed] up getting an entry card, so I think all of those aspects. We also need to address the most critical areas and then, so even like, if someone comes into the building and they don't have a recognised face, they are not authenticated from a perspective of working here, and all of those things. So drive the culture around people, processes, technology from a security perspective. You don't have to have everyone in a room and take up everyone's time, but short straight out effective videos which, the right education, keeping in mind the level and the current culture that we're in, [be]cause also we are going through a level of restructuring. So at the same time people may not be as cognisant and focused as they would normally be, so in these sort of scenarios people might even be a little more careless or loose things more or do things they might not normally do” (Appendix B12, IQ 1.3.3).

Finding 23: The current format of security education is not effective

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

Some participants (P3, P4 and P7) feel that awareness could be one of the contributory factors, because users do not understand the important role they have

to play in terms of IT security in an organisation. P4 elaborated that they need to place the responsibility on the users:

> "Look, I think it is more the awareness of people. I, we can make them aware and even put some of the responsibility onto them, then they would like if I… it might be a stupid example, but in the past we had people, they change their password now and then 10 minutes down the line they still forget it. I change my password today and I forgot it. Anyway, you normally pick up, you get the same type of people with the same people calling for the same thing, and I always say, if we had to charge you people to change your password, Engen would make a lot of money. I think many people will probably be on about it, but that it might even stop them from forgetting their password" (Appendix B4, IQ 1.3.4).

P7 is in agreement that that there should be more awareness on responsibility because the very nature of a human being is to be curious; however, this curiosity can lead to staff opening the wrong emails. According to P11, security in general is complex to understand and it is the responsibility of the IT Security staff to simplify the message around security. P11 stated that,

> "Security is complex and we [are] not going to change. There is no point in, I don't think we should be trying to engage the user and explaining what encryption is and how they should encrypt it. I think they [are] not going to understand it, they [are] just going to miss it and we are not going to change the culture at all" (Appendix B11, IQ 1.3.4).

However, P12 is of the opinion that users are resisting the changes coming from the IT Security department, and because of this negativity, they do not want to change their behaviour towards the IT security department personnel us. P12 said:

> "I think its people's education and awareness of the importance of security and the impact thereof. I was going to say change, but the resistance to change is any times because of the fact of who caused it, because they don't actually understand the importance of things. So when someone is sitting at the depot and they need to process something on an application, are they aware that if they do something wrong on that application that they could actually be fired when it looks like they [are] causing fraud or whatever case people might do legitimate mistakes, and this is why it's so important even when someone has access to systems that they know what they [are] doing, because you can actually create a massive issue, even business disruption, and all of those things. So I think the most important thing is the education, effective education and awareness, to the right role players starting from the top" (Appendix B12, IQ 1.3.4).

Finding 24: The current IT security processes are difficult for the users to understand

4.4.2 Summary of the findings

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

See Table 4.5 for the findings of RSQ 1.1.

Table 4.5: Findings of RSQ 1.1

Finding No.	Finding
Finding 1	Users do not have the necessary knowledge of IT security and need to be educated on this topic
Finding 2	It is not clear what risks the department is protecting the organisation against
Finding 3	Users do not know what their responsibilities are towards information security
Finding 4	Security communication is not recognised and understood
Finding 5	Users are not aware of the risk of sharing passwords among one another
Finding 6	Users are not accountable for security breaches, as there is no repercussion when they do something wrong
Finding 7	Users do not fully understand the different ways hackers are attempting to breach the company's network
Finding 8	Users do not take ownership; they leave the decision to the IT department
Finding 9	Users need to take responsibility and should not pass the blame to IT only
Finding 10	There are no security policies and procedure training for new employees
Finding 11	Too many silos in departments is part of the problem why it is so difficult for users to change
Finding 12	Some older employees are not open to new ideas and resist any new changes
Finding 13	There are too many processes inside the organisation

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

Table 4.6 summarises the findings for RSQ 1.2.

Table 4.6: Findings of RSQ 1.2

Finding No.	Finding
Finding 14	No security communication compliance records are kept
Finding 15	A different communication strategy than what is currently being used inside the organisation is needed
Finding 16	No or little assessments are done after security messages have been delivered
Finding 17	Users who do not follow the security policies should be punished as part of consequence management

Finding 18	Key performance indicators in terms of information security are not part of the user's job description and appraisal system
Finding 19	There is a lack of training and as a result, users are still clicking and opening phishing emails
Finding 20	There are budget constraints on security training and awareness

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

The findings for RSQ 1.3 are summarised in Table 4.7.

Table 4.7: Findings of RSQ 1.3

Finding No.	Finding
Finding 21	There is a lack of management buy-in when it comes to security
Finding 22	The user's perception of what the Information Security department is doing needs to change
Finding 23	The current format of security education is not effective
Finding 24	The current IT security processes are difficult for the users to understand

4.4.3 Summary of findings and theme development

Table 4.8 presents the findings and related themes linked to RQ1.

Table 4.8: Finding and related themes for RQ1

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?			
Finding		**Category**	**Themes**
Finding 1	Users do not have the necessary knowledge of IT security and need to be educated on this topic	Information security education	User awareness, training and education
Finding 2	It is not clear what risks the department is protecting the organisation against	Risk management education	User awareness, training and education
Finding 3	Users do not know what their responsibilities are towards information security	User responsibility	User management
Finding 4	Security communication is not recognised and understood	User compliance	Compliance and monitoring
Finding 5	Users are not aware of the risk of sharing passwords among one another	Password management education	User awareness, training and education
Finding 6	Users are not accountable for security breaches, as there is no repercussion when they do something wrong	User accountability	User management

Finding 7	Users do not fully understand the different ways hackers are attempting to breach the company's network.	User education	User awareness, training and education
Finding 8	Users do not take ownership; the leave the decision to the IT department	User ownership	User management
Finding 9	Users need to take responsibility and should not pass the blame to IT only	User responsibility	User Management
Finding 10	There are no security policies and procedure training for new employees	Induction Training	Induction training
Finding 11	Too many silos in departments is part of the problem why it is so difficult for users to change	Department silos breakdown	Change management
Finding 12	Some older employees are not open to new ideas and resist any new changes	Change management	Change management
Finding 13	There are too many processes inside the organisation	Process simplification	Process simplification
Finding 14	No security communication compliance records are kept	User compliance	Compliance and monitoring
Finding 15	A different communication strategy than what is currently being used inside the organisation is needed	Communication strategy	Communication strategy
Finding 16	No or little assessments are done after security messages have been delivered	User compliance	Compliance and monitoring
Finding 17	Users who do not follow the security policies should be punished as part of consequence management	Consequence management	User management
Finding 18	Key performance indicators in terms of information security are not part of the user's job description and appraisal system	Appraisal system	User management
Finding 19	There is a lack of training and as a result, users are still clicking and opening phishing emails	User training	User awareness, training and education
Finding 20	There are budget constraints on security training and awareness	Budget allocation	Top management support
Finding 21	There is a lack of management buy-in when it comes to security	Management buy-in	Top management support
Finding 22	The user's perception of what the Information Security department is doing needs to change	Information security education	User awareness, training and education
Finding 23	The current format of security education is not effective	Communication strategy	Communication strategy
Finding 24	The current IT security processes are difficult for the users to understand	Process simplification	Process simplification

4.5 Themes

In this chapter, information of the case used for the research is discussed. Data from the interviews (consisting of 13 interview questions and answered by 12

participants) conducted during the research process, are analysed. Twenty four (24) findings are identified based on the analysis of the data. Seven (7) themes are developed from the (24) findings. These seven themes are as follows:

i) User awareness, training and education
ii) User management
iii) Compliance and monitoring
iv) Change management
v) Process simplification
vi) Communication strategy
vii) Top management support

Table 4.9: Themes developed based on RQ1 and RSQs

Research questions	Themes
RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?	**User awareness, training and education**
IQ 1.1.1: Do you feel the users adhere to the requirements set out by your department?	User awareness, training and education
IQ 1.1.2: According to you, do you think users know what their responsibility is towards information security?	User management Compliance and monitoring
IQ 1.1.3: According to you, do you feel users are aware of the risk of not following the information security procedures?	User awareness, training and education User management
IQ 1.1.4: According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?	User management
IQ 1.1.5: What are the greatest challenges with instituting an information security culture at Engen?	Induction training Change management Process simplification
RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?	**Communication strategy** **Compliance and monitoring**
IQ 1.2.1: According to you, does your department provide adequate information security training to your users to inform them during changes?	Compliance and monitoring
IQ 1.2.2: According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?	Communication strategy Compliance and monitoring
IQ 1.2.3: Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?	User management
IQ 1.2.4: Do you feel Engen's current security awareness training is effective?	User awareness, training and education Top management support

Research questions	Themes
RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?	**Top management support**
IQ 1.3.1: According to you, what processes can be created inside the organisation to institutionalise a culture of security?	Top management support
IQ 1.3.2: How would you describe the information security culture at Engen?	User awareness, training and education
IQ 1.3.3: Please indicate and give examples of how information security culture can be created in your organisation.	Communication strategy
IQ 1.3.4: What do you consider being the main contributory factors to create an effective information security culture at Engen?	Process simplification

4.6 Summary of the findings and themes

4.6.1 Findings and interview questions

Table 4.10 shows the relationship between the theme, findings, research sub-question, and research question. The themes, *user awareness training*, *user management*, *compliance and monitoring*, *change management*, *process simplification*, *communication strategy,* and *top management support*, answer RQ1.

Table 4.10: Findings per theme

Theme	Findings	RSQ	RQ
User awareness training and education	1, 2, 5, 7, 10, 9, 22	1.1, 1.2, 1.4, 1.11, 1.14	1
User management	3, 6, 8, 9, 17, 18	1.3, 1.4, 1.5, 1.10	1
Compliance and monitoring	4, 14, 16	1.3, 1.7, 1.8, 1.9	1
Change management	11, 12	1.6	1
Process simplification	13, 24	1.6, 1.16	1
Communication strategy	15, 23	1.7, 1.9, 1.15	1
Top management support	20, 21	1.11, 1.12, 1.13	1

Table 4.11 shows the summary of the number of findings derived per category and the total number of findings per theme.

4.6.2 Themes arranged according to the number of findings

Table 4.11: Themes arranged according to the number of findings

Theme	Category	No. of findings	Sum per category
User awareness training and education	Information security education	2	7

Theme	Category	No. of findings	Sum per category
	Risk management education	1	
	Password management education	1	
	User education	1	
	Induction training	1	
	User Training	1	
User management	User responsibility	2	6
	User accountability	1	
	User ownership	1	
	Consequence management	1	
	Appraisal system	1	
Compliance and monitoring	User compliance	3	3
Change management	Department silos breakdown	1	2
	Change management	1	
Process simplification	Process simplification	2	2
Communication strategy	Communication strategy	2	2
Top management support	Budget allocation	1	2
	Management buy-in	1	

4.7 Summary

Chapter 4 provided the background of the case for the research, herein referred to as the organisation. The organisation is one of the leading marketers of petroleum-based products and convenience services and has a presence in over 20 countries in sub-Saharan Africa and the Indian Ocean Islands.

For the purpose of the research, 12 participants in the Information Technology department have been interviewed. The participants included managers, SAP specialists, IT Security specialists, and risk practitioners. All of the participants have some experience in IT.

Based on the responses of the interviewees and the analysis of their answers, findings were derived for each interview question through transcribing, summarising and categorising the data, as discussed in Chapter 3. From the 24 findings, seven themes have been identified. The themes are:

i) User awareness training and education
ii) User management
iii) Compliance and monitoring
iv) Change management
v) Process simplification

vi) Communication strategy
vii) Top management support

In Chapter 5, the themes are discussed and linked to the research questions and the aim of the study.

5. CHAPTER 5: DISCUSSION

5.1 Introduction

From the findings described in Chapter 4, seven themes have been identified. The themes are:

i) User awareness training and education
ii) User management
iii) Compliance and monitoring
iv) Change management
v) Process simplification
vi) Communication strategy
vii) Top management support

In Chapter 5, the themes are discussed and linked to the research questions and aim of the study. At the end of the chapter, a summary is given. For the ease of reading, the problem statement, research questions, and the aim of the study are listed below:

Problem statement: The failure to institutionalise an information security culture inside an organisation will cause the continued occurrence of security breaches, costing the organisation reputational as well as financial losses.

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

Aim of the study: To explore how an information security culture can be institutionalised inside the petroleum organisation in the Western Cape.

5.2 The themes

5.2.1 Theme 1: User awareness training and education

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

To answer RSQ 1.1, most participants are aware of the notification emails that are sent to the users on a monthly basis. This type of communication has been discontinued after a new CEO came on board and felt that only business related emails should be communicated via the email system. Because of this, the IT Security department replaced the email notification with security awareness posters across the organisation. Despite this initiative, some participants felt users are still not sufficiently educated on information security. This has proven to be true, because the department ran a phishing simulation in the organisation and some users still opened the phishing emails. P8 said:

> "I don't think the training is adequate. I don't think users is educated enough as to what changes is happening, the education of the users, because you can inform them about the following changes the firewalls make, the following changes the web makes, the following changes etc., and all the changes, but if they are not educated and fully understanding what does it change and what does it do for Engen, then obviously that will not salt to them. Then it's no use. I think at this stage we need to move more on education…" (Appendix B8, IQ 1.2.1).

P8 further explained that if management makes more funds available for security awareness training, the department can look at other forms of training, for example multimedia video training. According to Tang et al. (2015), irrespective of how sophisticated the technologies are, without the necessary awareness of information security by employees, information losses will continue to occur.

Da Veiga and Martins (2015) explain that information security training is seen as one of the most effective ways for businesses to protect their information resources. From this research, it is evident that user awareness in the form of email communication and posters are being conducted, however, there is no record of whether the users open and understand the sent messages. P9 stated that compliance needs to be measured to verify if users understand these messages: "I think any training needs to have a measurement of compliance, so we can't just deliver training and expecting the user base to consume it and be under the impression or expectation that we have successfully delivered training. So we definitely have to follow up that training with compliance…" (Appendix B11, IQ 1.2.1).

Another concern is how the awareness messages are communicated to none-head office staff such as the truck drivers, because currently the message is only being sent to internal computer users. P7 said:

> "At the moment the one that are [sic] more effective is the in-house which [has] already been done, but additionally, I don't think in terms of... remember even all the users that are all on the road… they can mainly access emails so basically they do read emails. We cannot emphasise more that we are actually doing by emails and posters everywhere" (Appendix B7, IQ 1.3.1).

While IS security training suggests the distribution of messages on the importance of IS security compliance through e-mail and posters, additional security training methods need to be looked at to enhance the effectiveness of the security training. P3 said:

> "Maybe [a] day for security awareness and maybe that's another outlook, getting people interested and getting them phoning us. I think their silence is actually creates that wall. Nobody's actually interested in 'you will do this and you will do that'. I think it is both, definitely. You want people to engage with you and you want people to be interested in security, otherwise they will never actually use security. The video will be multimedia" (Appendix B3, IQ 1.3.4).

One aspect that most participants do agree on is that IS security training needs to be reintroduce during the induction process of all new employees. P6 proposed a section to be included in the Engen induction course where policies are discussed and where employees are briefed on what to expect if they breach the company's security so that they cannot later say they did not know of the consequences.

It seems that there is still a lack of user awareness, even after training has been conducted. The need for continuous training has been expressed and resonates with what Schlienger and Teufel (2005) say, namely that information security culture is ultimately visible in the artefacts, beliefs and values of an organisation. Information security induction training could be visible as an artefact. In the literature, it is found that users are the weakest link when it comes to information security (Karlsson & Hedstrom, 2014; Bresz, 2004; Mitnick & Simon, 2002).

5.2.2 Theme 2: User management

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

To answer RQ1, most participants feel that after all that has been done by the IT Security department, users are still not taking the necessary ownership and responsibility when it comes to IT security. Some participants feel it may be the

culture of the organisation that is allowing this, and some users have an 'I do not care attitude'. P3 said that in one case, a user from the audit team wanted to force her to bypass the controls and grant access to the resource.

According to Alnatheer et al. (2012), one of the factors to institute a culture of security in an organisation is security ownership. Without ownership, it is difficult to create a culture of security within the organisation. Currently there is little ownership within the organisation, as can been seen in the above example. Another participant feels it is usually the users who are a bit longer at the organisation that resist the changes (see theme 4). Participant 12 said: "Definitely resistance to change. I think people especially at Engen, some of them have been in there jobs for 20, 30 years and I'm not only referring to them because there's people that's been here for 2, or 3 years also, but I think historically our organisation has done things a certain way now" (Appendix B12, IQ 1.1.5). Layton (2005) is of the opinion that users should be asked to change their behaviour and understand the risks if they consistently behave in a certain way.

Some participants are of the opinion that there are departmental silos in the organisation and that each department is only looking out for itself. P2 argued that, "the biggest challenges, as I have mentioned before, is of the silos that is [sic] here. The people protect the environment tremendously. They do not want our departments to scratch out their environment or they are very protective of their environment" (Appendix B2, IQ 1.1.5). From a user management perspective it is essential that these silos are broken down, as they will negatively affect an organisation-wide security culture. In order to break down these silos, Kabay (2002) suggests that users who display "secure attitudes" should be praised, and that users who do not show an improved attitude towards the importance of security should be challenged in private.

5.2.3 Theme 3: Compliance and monitoring

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

In an endeavour to answer RSQ 1.2, participants are clear that one cannot just send out security awareness notifications without putting the necessary measures in place to verify the effectiveness thereof, otherwise the IT Security department will simply assume or tick off the box that security awareness is in place. P11 stated that any type training should contain some measurement to determine successful delivery of the material. The IT Security department should therefore follow up after

training has been completed to verify compliance. Without compliance checking it is difficult to measure the success of a security awareness campaign.

Continuous monitoring of the compliance processes is needed to ensure an effective and efficient compliance culture.

5.2.4 Theme 4: Change management

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

In an endeavour to answer RSQ 1.2, Schein (2009) recommends an organised change management process to facilitate the creation of an information security culture change inside an organisation (see theme 2).

In order to ensure an effective information security culture in the organisation, change management principles from the information security change framework (Alhogail & Mirza, 2014) can be adapted to guide and support the effective implementation thereof. The principles are presented in Figure 5.1.

Figure 5.1: Information security culture change management principle
(Al Hogail & Mirza, 2014:10)

According to the research, P12 feels that users who have been a bit longer in the organisation are resisting any new changes coming from the Security department. In order to win over these users, the necessary buy-in from the staff members is

needed to create small wins. According to P12, people who have been working for 20 to 30 years are set in there ways and used to do things in a certain way. This resistance is especially evident when implementing new measures or sharing information – there seems to be no buy-in from top management and some senior managers do not seem to understand the importance of information security.

5.2.5 Theme 5: Process simplification

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

In an endeavour to answer RSQ 1.3, the participants argued that the organisation has too many processes in place and this can cause delays for the engineers and the users. P2 said:

> Something else I've noticed also is processes – this company is very process-driven and sometimes these processes have an impact on the actual work that needs to be done because processes take time. Because approvals needs [sic] to be done, it goes through a whole long list of approvals, goes to a whole list of testing, a whole list of everything before the actual work gets done. So processes need to be re-looked at this company through maybe streamline it and make it more effective. For now, that's the only thing" (Appendix B2, IQ 1.1.5).

P12 agrees with this. P12 said that the organisation has good governance, processes and controls in place. P5 indicated that the processes need to be simplified: "I actually think there are too many processes for similar things, so I actually would say instead of creating a process, you should change things and simplify it, to answer your question" (Appendix B5, IQ 1.3.1).

In order to be effective as a department, processes need to be simplified. If users want to report incidents to the IT Security department or if they opened any suspicious email, the department needs to have simple processes in place to assist the users. If not, users will not report these incidents or will simply ignore the department. According to Zakaria (2006), there should be a good peer relationship between the user and the department to promote information security knowledge sharing. The author further states that this knowledge should include recognition of what is reward and punishment in terms of information security matters (Zakara, 2006).

5.2.6 Theme 6: Communication strategy

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

To answer RSQ 1.2, there should be a process to make IS security communication a "time-divergent" process in the organisation. Helokunnas and Kuusisto (2003) agree with this and state that time-divergent communication can be used to promote knowledge of information security among employees. Time-divergent communication relates to the communication of information security activities conducted in the past, present and future. Thus, in order to motivate users to comply with IS security policies, IS security training and awareness should be integrated with the normal business communication of the organisation. Another important point to note is that when the organisation transitioned from one CEO to the next, the new CEO did not want the IT Security department to send out any electronic awareness communication as he believes only business-related messages are supposed to be sent via email. The IT Security department therefore had to change their communication strategy; in the past they distributed awareness communication once a month via email with a different topic each time, but now the messages have to be displayed on a security poster.

There is currently no measure in place to verify the effectiveness of the current communication strategy, thus some participants feel they are not doing enough to spread the message of security, and that more can be done. P12 said: "I don't think they are providing adequate training now. I think they maybe do provide a level awareness through communications but I don't think they provide adequate training around security measures…" (Appendix B12, IQ 1.2.1). However, some participants feel enough is being done, especially with the resources available. P1 suggested that posters should be used to get the message across. P8 argued that the messages need to be more practical and "bring it home" for the users. The argument of Beautement et al. (2008) is supported by this finding. Security messages can be more meaningful and interesting if it is short, and presentation sessions should not exceed ten to fifteen minutes.

5.2.7 Theme 7: Top management support

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

To answer RSQ 1.1, top management should support the local Information Security department and rally behind them when any communication regarding information

security is sent throughout the organisation. An example of this is when security awareness posters are being designed – it can be signed by the CEO to endorse the work the department is doing. Knapp et al. (2006) are of the opinion that top management support positively influences security culture.

According to Lim et al. (2009), an information security culture does not normally form an integral part of the organisational culture, because security managers frequently have difficulty in obtaining sufficient funding from management to implement information security practices. Information security measures only involve a small group of employees to implement the security strategy of the organisation. This is evident in the case organisation as well. P8 is of the opinion that additional material can be purchased to strengthen the IT security message if management makes more funding available.

D'Arcy and Green (2009) agree that senior management support in an organisation is important in promoting security. Thus, senior management needs to show their support through active participation in the security activities of the IT Security department. Another way top management can show support is to provide the necessary funding for security projects. P12 said that one way management could show their support of IT security is by making funds available: “If management is not making funding available for certain things when some things are not highly effective and it’s important, then it rather sends the wrong message” (Appendix B12, IQ 1.3.2).

Management seems to be busy with business issues other than security, and they often display non-compliance with information security instructions. This gives the impression that management does not consider IS security to be important, which has a negative impact on motivation to comply with the instructions.

5.3 The proposed guidelines

The following guidelines consist of components that could assist the organisation in institutionalising a culture of security:

i) Awareness

- Employees should be aware of the need for information security
- Employees should know what they can do to keep computer systems safe from intruders

ii) Responsibility

- Employees should know their responsibility towards information security

- Both the employees and management are responsible for the security of information systems

iii) Response

- Employees should act in a timely manner to detect, prevent and respond to any information security incidents
- Employees should consult the Information Security department without the fear for retribution if they open any suspicious emails

iv) Reassessment

- The IT Security department should continuously assess the effectiveness of their security campaigns
- The necessary security campaign modifications must be made in order to institute a culture of security

By adopting and enforcing the guidelines mentioned above, the organisation will institute a culture of security.

5.4 Answering the research questions

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

From the research, factors have been identified on both the user and the IT Security department's side. The method used to conduct user awareness is highlighted throughout the research and the department needs to improve on this. As part of the improved process, the department should do compliance checks to verify the effectiveness of the security awareness programmes. Other factors that were revealed during the research are the silos in departments that cause some employees to always be negative about information security, buy-in from management, and the need for more funds.

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

Users do not have the necessary knowledge of information security, and because of this they are not accountable and do not know what their responsibilities are. It has been found that some older employees are not open to new ideas and are resisting new changes. Users do not take ownership when it comes to information security and leave the decision in the hands of the IT department.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

Although the organisation has a change advisory board process, these processes seem to be too complex and much simpler processes are needed. Messages are sent via email and some users feel they simply receive too many emails, which causes them to ignore these messages. Thus, a more effective communication strategy needs to be designed where measurements are put in place to obtain continuous feedback from the users.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

From the research it is evident that the communication processes between the users and the IT Security department need to be simplified so that the security message is clear and concise. A new assessment process needs to be created after each security awareness programme to verify the effectiveness of the programme.

5.5 The aim

The aim of this research is to explore how an information security culture can be institutionalised within a petroleum organisation in the Western Cape.

The divergence that exists between technology and users need to be addressed. Although employees do use the technology, they need to take ownership of what computer equipment they are using, and how they use it. The Information Technology department, especially the Information Security section, should not be seen as the enemy for not allowing users to browse the Internet. The same security mindset that users have at home or when visiting the bank should also be applied at work. The aim is achieved by applying the proposed guidelines.

5.6 Summary

Chapter 5 discussed the themes identified in Chapter 4 and elaborated on how each theme is linked to the research questions and the aim of the study. In order to address the research problem, one main research question has been developed, namely: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape? At the end of the chapter, the research question and sub-research questions were answered and the aim of the research was addressed. The next chapter (6) discusses the conclusions, recommendations, reflections and contribution of the research.

CHAPTER 6: CONCLUSIONS, RECOMMENDATIONS AND REFLECTION

Chapter 6 presents the conclusions, recommendations, a reflection on the research conducted, and the contribution of the research.

It is clear from this research that users do not know what their responsibility is towards information security, thus, they do not take ownership and are unaware of the risk posed by potential security breaches to the organisation. Although attempts have been made to communicate the security message via email and other communication methods, this has not been successful. Some users find it difficult to change their behaviour towards information security because of the company culture, of not being open to any new ideas, and because of silos in the different departments. It is very difficult to obtain buy-in from management, and limited funding is available to action the information security plan in the organisation. Users seem to have a 'do not care attitude' regarding information security and the department seems to be the enemy who is continuously putting security controls in place to block users from using the Internet.

6.1 Recommendations

The following recommendations are made after having considered all the findings and theme discussions:

i) Implement the proposed guidelines indicated in section 5.3 that have been developed for the organisation to follow in order to institute this information security culture.

ii) Change agents are needed in the organisation to change the culture. Use senior and middle management as the change agents and take them through an intensive security awareness training programme to obtain their much needed buy-in. Once this has been achieved, enable the management team to influence the team leaders and employees who are

iii) reporting to them. By doing this, the management can be used as change agents for security, and silos can be broken down within the organisation and between departments. The importance of information security should be conveyed to employees by management and not by the Information Security department.

iv) Run frequent compliance checks after each security awareness campaign to ensure the effectiveness of the security awareness programmes in the organisation. For example, run monthly phishing campaigns to verify who is still opening phishing emails and then focus on these individuals during follow-up campaigns. Additionally, run the same campaign only to the identified individuals before allowing them to advance to the next campaign. During a social engineering awareness campaign, acquire a third party company to call some users in order to determine who is still divulging the private information of the organisation. Identify these users and take them through additional training if needed. Monitor the success of these interventions and apply this to other topics related to information security.

v) Change the approach of how training is currently conducted by altering the training format on a monthly basis, and determine what is acceptable to the users by sending out surveys and obtaining continuous feedback from them after each campaign. Users need to be trained on a continuous basis and all new employees must be made aware of their responsibility during induction training. It is also important that a culture of security is instituted by the organisation in which employees understand that ICT security is not the responsibility of ICT professionals only; it starts with the users.

vi) Break down the silos in an organisation through facilitating continuous discussions between the end-user and the departments, explaining the reason why security measures need to be in place and showing real examples of how other organisations were compromised.

6.2 Reflection on the study

The research followed a case study approach, limited to a specific oil and gas organisation in the Western Cape. The research results are as accurate as possible and based on the interview answers obtained from the 12 participants. It must be emphasised that the results cannot be generalised, as it is unique to the organisation.

Various challenges were experienced before and during the interviews, for example, the organisation was going through a restructuring process and one of the participants interviewed for this study is no longer working at the organisation.

Secondly, the researcher is unsure of how the restructuring process influenced the truthfulness of the answers provided during the interview process although every effort was made to get as close to the truth as possible.

In some cases, participants were in a rush to do the interview and simply answered the questions in as short as possible time without elaborating. This created a challenge as some of these participants are senior staff members that could have enhanced the research with more of their insights. In retrospect, these participants should have been re-interviewed.

6.3 Suggestions for future research

It is important to realise that institutionalising a culture of security in an organisation is a long-term process. This process needs to be on-going due to the fast evolving nature of information technology; such a process would need continuous revision.

The findings of the research open the doors to more questions that need to be answered, including, “how does the security culture of start-up organisation differ from a more structured organisation such as the oil and gas company?”, and “do younger employees conform much easier when an organisation wants to institute a culture of security?” Further research on the same topic at other oil and gas companies in South Africa can be conducted as well.

It is recommended to further investigate how information security restrictions imposed on employees influence the culture of security in an institution.

6.4 Limitation of research

Some limitations of the study should be noted. The sample size of twelve is relatively small, so one should guard against generalisation when interpreting the findings. The study has been conducted at the head offices where the researcher is working, and the researcher had no access to the regional and international business division offices of the organisation.

6.5 Summary

If an information security culture is not institutionalised in the organisation, it will be only a matter of time before the organisation is breached by people or via technology, which will cost the organisation reputational and financial losses.

Some of the top findings derived from the research as summarised as follows: Firstly, although users are using the company’s computer resources every day, they are not clear on the risks the organisation is facing when it comes to information

security. Thus, they do not know what their responsibilities are and how hackers can target them to infiltrate the organisation's network. Secondly, information security is not part of the key performance indicators (KPIs) of the user's performance contract. Thirdly, the Information Security department does not conduct regular compliance checks to ensure the effectiveness of the current security training programme.

To answer the research question, "what the factors are affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?", the researcher found the user, management, and the Information Security department to be responsible.

Awareness, responsibility, response, and reassessment are some of the guidelines proposed to assist the organisation in instituting a culture of the security.

REFERENCE LIST

Adler, J., Demicco, M. & Neiditz, J. 2015. Critical privacy and data security risk management issues for the franchisor. *Franchise Law Journal,* 35(1):79-92.

Alfawaz, S., Nelson, K. & Mohannak, K. 2010. *Information security culture: a behaviour compliance conceptual framework.* Australia: QUT Digital Repository.

Al Hogail, A. 2015. Design and validation of information security culture framework. *Computer Human Behaviour,* 49:567-575.

Al Hogail, A. & Mirza, A. 2014. A framework of information security culture change. *Journal of Theoretical and Applied Information Technology,* 64(2):10.

Alnatheer, M., Chan, T. & Nelson, K. 2012. Understanding and measuring information security culture. *Proceedings*. Pacific Asia Conference on Information Systems (PACIS 2012).

Alnatheer, M. & Nelson, K. 2009. Proposed framework for understanding information security culture and practices in the Saudi context. *Proceedings*. 7th Australian Information Security Management Conference*,* Australia.

Babbie, E. 2012. *The practice of social research.* 13th ed. Australia: Wadsworth.

Babbie, E. & Mouton, J. 2001. *The practice of social research.* Cape Town: Oxford University Press South Africa.

Beautement, A., Sasse, M. & Wonham, M. 2008. The compliance budget: managing security behaviour in organisations. New Security Paradigms Workshop (NSPW). p.12.

Bengtsson, M. 2016. How to plan and perform a qualitative study using content analysis. *Nursing Plus Open 2,* 8-14.

Bhattacherjee, A. 2012. *Social science research: principles, methods, and practices*. University of South Florida (USF), Open Access Textbooks, Collection Book 3.

Bresz, F. 2004. People - often the weakest link in security, but one of the best places to start. *Journal of Health Care Compliance,* 6(4):57-60.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 34(3):523-548.

Cameron, K. & Quinn, R. 2011. *Diagnosing and changing organisational culture.* Revised ed. San Francisco: Jossey-Bass.

Chen, Y., Ramamurthy, K. & Wen, K. 2015. Impacts of comprehensive information security programs on information security culture. *The journal of Computer Information Systems,* 55(3):11-19.

Creswell, J. 2009. *Research design: qualitative, quantitative, and mixed approaches.* 3rd ed. California: Sage.

Da Veiga, A. 2016. Comparing the information security culture of employees who had read the information security policy and those who had not illustrated through an empirical study. *Information & Computer Security,* 24(2):139-151.

Da Veiga, A. & Eloff, J. 2010. A framework and assessment instrument for information security culture. *Computers & Security,* 29(2):1-12.

Da Veiga, A. & Martins, N. 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49:162-176.

D'Arcy, J. & Green, G. 2009. The multifacted nature of security culture and its influence on end user behaviour. *Proceedings.* IFIP TC8 international workshop on information systems security research, May 29-30, Cape Town, South Africa: 57-145. USA: IFIP.

Deloitte, Touche & Tohmatsu. 2005. *Deloitte.* [Online]. Available at: http://www2.deloitte.com/za/en.html. [Accessed: 24 September 2016].

Dillard, J., Rigsby, F. & Goodman, J.T.C. (2004). The making and remaking of organization context: Duality and the institutionalization process. Accounting, Auditing & Accountability Journal, 17(4). 506-542. doi:10.1108/09513570410554542

Dimitriadis, C. 2011. Information security from a business perspective. *ISACA Journal,* 43-48.

Dunsmuir, L. & Finkle, J. 2015. *Reuters.* [Online]. Available at: http://www.reuters.com/article/usa-cybercrime-justice-idUSL1N0W81QY2015030. [Accessed: 22 September 2016].

Fichman, R., 2011. The role of Information Systems in healthcare: current research and future trends. *Information Systems Res,* 22(3):419-428.

Finch, J., Furnell, S. & Dowland, P. 2003. *Assessing IT security culture: system administrator and end-user perspectives.* Proceedings*. ISOneWorld2003,* United Kingdom. Network Research Group.

Gebrasilase, T. & Lessa, L. 2011. Information security culture in public hospitals: the case of Hawassa referral hospital. *The African Journal of Information Systems,* 3(3):1-16.

Hafizah, N. & Ismail, Z. 2016. Information security culture in Healthcare Informatics: a preliminary investigation. *Journal of Theorectical and Applied Information Technology,* 88(2):202-209.

Harman, K 2002. Merging divergent campus cultures into coherent educational communities: Challenges for higher education leaders. Higher Education, 44(1): 91-114.

Helokunnas, T. & Kuusisto, R. 2003. Information security culture in a value net. *Proceedings*. IEEE International Engineering Management Conference, Albany, New York.

Herold, R. 2011. *Managing an information security and privacy awareness and training program.* Boca Raton: Taylor and Francis Group.

Holtfreter, R. & Harrington, A. 2015. Data breaches trends in the United States. *Journal of Financial Crime,* 22(2):242-260.

Huang, E. & Chuang, M. 2007. Extending the theory of planned behaviour as a model to explain post-merger employee behaviour of IS use. *Computers in Human Behaviour,* 23(1):240-257.

ISACA. 2011. *Creating a culture of security.* [Online]. Available at: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx. [Accessed: 28 March 2017].

ISO. 2013. *Online browsing platform.* [Online]. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. [Accessed: 26 July 2016].

Kabay, M. 2002. *Computer security handbook.* 4th ed. s.l.:John Wiley & Sons.

Karlsson, F., Astrom, J. & Karlsson, M. 2015. Information security culture - state of the art review between 2000 and 2013. *Information & Computer Security,* 23(3):246-285.

Karlsson, F. & Hedstrom, K. 2014. *End user development and information security culture.* Greece: CI International.

Knapp, K. & Marshall, T. 2006. Information security: management's effect on culture and policy. *Information Management Computer Security,* 14(1):24-36.

Knapp, K., Marshall, T., Rainer, R. & Ford, F. 2006. Information security: management effect on culture and policy. *Information and Computer Security,* 14(1):24-36.

Layton, R. & Watters, P. 2014. A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications,* 19(6):321-330.

Layton, T. 2005. *Information security awareness: the psychology behind the technology,* s.l.: AuthorHouse.

Liginlal, D., Sim, I. & Khansa, L. 2009. How significant is human error as a cause of privacy breaches. *Computer Security,* 28(3-4):215-228.

Lim, C.J., Maynard, S. & Ahmad, A. 2009. *Exploring the relationship between organisational culture and information security culture.* Perth: SECAU.

Liu, V., Musen, M. & Chou, T. 2015. Data breaches of protected health information in the United States. *JAMA,* 313(14):1471-1473.

Malcomson, J. 2009. *What is security culture? Does it differ in content from general organisational culture.* Zurich: Security Technology.

Maree, K. 2007. *First steps in research.* Pretoria: Van Schaik.

Martins, A. & Eloff, J. 2002. *Assessing information security culture.* South Africa: Springer. p. 14.

Maynard, S., Ruighaver, A. & Chia, P. 2002. *Exploring organisational security culture: developing a comprehensive research model. Proceedings.* IS ONE World Conference, Australia.

Mitnick, K. & Simon, W. 2002. *The art of deception: controlling the human element of security.* United States of America: Wiley.

Mkansi, M. & Acheampong, E.A. 2012. Research philosophy debates and classifications: students' dilemma. *Electronic Journal of Business Research Methods*, 10(2):132-140.

Myers, M. 2013. *Qualitative research in business & management.* 2nd ed. London: Sage.

Neuman, W. 2006. *Social research methods: qualitative and quantitative approaches.* 6th ed. USA: CiteUlike.

Neuman, W. 2011. *Social research methods: qualitative and quantitatvie approaches.* 7th ed. Boston: Pearson/Allyn and Bacon.

Ngo, L., Zhou, W., Chonka, A. & Singh, J. 2009. Assessing the level of IT security culture improvement: results from three Australian SME's. *Proceedings*. 35th Annual Conference of IEEE Industrial Electronics (IECON): 3189-3195.

Ngo, L., Zhou, W. & Warren, M. 2005. *Understanding transition towards information security culture change. Proceedings.* The 3rd Australian Computer, Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science, Perth, Australia: 67-73.

Obalola, M. & Adelopo, I. 2012. Measuring the perceived importance of ethics and social responsibility in financial services: a narrative-inductive approach. *Social Responsibility Journal,* 8(3):1-17.

O'Donovan, G. 2006. *The corporate culture handbook: how to plan implement and measure a successful culture change.* Ireland: The Liffer press, Ashbrook House.

Okere, I., Van Niekerk, J. & Caroll, M. 2012. Assessing information security culture: a critical analysis of current approaches. *Proceedings*. IEEE conference on Information Security of South Africa (ISSA), South Africa.

Oost, D. & Chew, E. 2007. *Investigating the concept of information security culture*. University of Technology Sydney, School of Management (UTS):12. [Online]. Available: https://pdfs.semanticscholar.org/c20d/3e00529d58bebc52bd7c59abe5db3d7a63af.pdf. [Accessed: 31 May 2018].

Padayachee, K. 2012. Taxonomy of compliant information security behaviour. *Computer Security,* 31(5):673-680.

Ponemon, L. 2016. *2016 Cost of data breach study,* Michigan: IBM.

Puhakainen, P. & Ahonen, R. 2006. *A design theory for information security awarenss.* PhD Thesis, University of OULU.

PWC. 2016. *The global state of information security,* USA: PWC.

Ramachandran, S. 2008. *Information security cultures of four professions: a comparative study.* 41st International Conference of System Science, Hawaii.

Resnik, D. 2015. *What is ethics in research & why is it important?* [Online]. Available at: https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm. [Accessed: 15 May 2018].

Riley, M., Elgin, B., Lawrence, D. & Matlack, C. 2014. *Bloomberg.* [Online]. Available at: http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data#p2. [Accessed: 24 September 2016].

Romanosky, S., Hoffmann, D. & Acquisti, A. 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies,* 11(1):74-104.

Ruggiano, N. & Brown, E. 2013. Adding home health care to the discussion on health information technology policy. *Home Health Care Service Quarterly,* 32(3):149-162.

Sapsford, R. & Jupp, V. 1996. *Data collection and analysis.* London: Sage.

Saunders, S., Lewis, P. & Thornhill, A. 2009. *Research methods for business students.* 5th ed. UK: Pearson Educational.

Schein, E. 2009. *The corporate culture survival guide.* San Francisco: Jossey-Bass.

Schlienger, T. & Teufel, S. 2003. *Analysing information security culture: increased trust by an appropriate information security culture.* Guatemala: IEEE.

Schlienger, T. & Teufel, S. 2005. Tool supported management of information security culture. *Proceedings.* IFIP Internation Information Security Conference, Japan.

Scott, W.R. (2008). Approaching adulthood: The maturing of institutional theory. Theory and Society, 37(5), 427-442. doi: 10.1007/s11186-008-9067-z

Shedden, P., Ahmad, A. & Ruighaver, A. 2006. Risk management standard-the perception of ease of use. *Proceedings.* Fifth Annual Security Conference, Las Vegas.

Sherwood J., Clark, A. & Lynas, .D. 2005. *Enterprise security architecture. A business-driven approach.* Berkeley: CMP Books.

Simone, JV 2009. Institutional Culture. Oncology Times, 31(5):5-6.

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. 2014. Variables influencing information security policy compliance. *Information Management & Computer Security,* 22(1):1-29.

Symantec. 2016. *itnewsafrica.* [Online]. Available at: http://www.itnewsafrica.com/2016/07/8-8-million-south-africans-have-fallen-victim-to-cybercrime/. [Accessed: 28 July 2016].

Tang, M., Li, M. & Zhang, T. 2015. The impacts of organisational culture on information security culture: a case study. *Journal Information Technology and Management*, 17(2):179-168.

Tessem H.M. & Skaaraas K.R. 2005. *Creating a security culture.* [Online]. Available at: http://www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015-022.pdf. [Accessed: 5 May 2018].

Thomas, D. 2003. A general inductive approach for qualitative data analysis. *American Journal of Evaluation,* 27(2):237-246.

Thomson, K. & Van Niekerk, J. 2012. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security,* 20(1):39-46.

Tipton, H. & Krause, M. 2007. *Information security management handbook.* 6th ed. London: Auerbach.

Van Niekerk, J.F. 2005. *Establishing an information security culture in organisations: an outcomes based education approach*. Master's dissertation, Nelson Mandela Metropolitan University, Port Elizabeth.

Van Niekerk, J. & Von Solms, R. 2006. Understanding information security culture: a conceptual framework. *Proceedings*. The ISSA 2006 from Insight to Foresight Conference, 2006, Balalaika Hotel, Sandton, South Africa, 5-7 July.

Van Niekerk, J. & Von Solms, R. 2010. Information security culture: a management perspective. *Computers & Security,* 29(4):476-486.

Vance, A., Lowry, P. & Eggett, D. 2013. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems,* 29(4):263-290.

Verton, D. 2001. Companies aim to build security awareness. *Computerworld,* 11(2).

Wahyuni, D. 2012. The Research design maze. Understanding paradigims, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, 10(1):69-80. Winter.

Wilson, J. 2013. *Essential of Business Research: A guide to doing your research project*. 2nd ed. London, United Kingdom: Sage Publications.

Woodhouse, S. 2007. *Information security: end user behaviour and corporate culture.* s.l., s.n.

Wook, K., Peiying, Y. & Junjie, Z. 2015. Detecting fake anti-virus software distribution webpages. *Computer Security,* 49:95-106.

Yin, R. 2003. *Case study research: design and methods.* 3rd ed. Thousand Oaks, CA: Sage.

Yin, R. 2014. *Case study research: design and methods.* 5th ed. USA: Sage.

Zakaria, O. 2006. *Internalisation of information security culture amongs employees through basis security knowledge.* Surrey: Springer.

APPENDIX A: INTERVIEW GUIDE TEMPLATE

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

IQ 1.3.2: *How would you describe the information security culture at Engen?*

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

APPENDIX B1: INTERVIEW ANSWERS OF PARTICIPANT 1

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I have to look at that question in two parts, right, so for one, do I think they adhere to it? They are kind of forced to, that is based on the controls that we put in place so they have to adhere to it. In saying that, if there is an opportunity for them to bypass some of the controls, I believe that they would use this opportunities and this is specifically around things like the USB devices where they do not want the USB devices encrypted with BitLocker. And if there was a way for them to turn that off, copying and use the data and copy the data onto the USB devices, I believe that they would go ahead because they would find the control that we put in place probably too restrictive and I believe that in their minds they believe it is too restrictive.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

The role that they have to play do I believe it. I don't think so and I don't think so because I think that if they could bypass the controls that's been put in place they would bypass it. So I don't think they will adhere to it.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

No, and the reason why I say that is that I think a lot of the controls that's put in place is line to restrictive. No, I don't think that they are aware of the risk and I think the main reason for that is they haven't personally, I think, experience or been subjected to somebody that has gone through a security breach where a machine has been compromised or even some credentials has been compromised, stolen. I don't think that that they are aware of it.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

I think they would take ownership because if something, if a breach should occur due to them bypassing the control, they would need to take ownership and have to put up their hand and say I did this.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

It is people's perceptions. There will always be a none-positive outlook from the user on security and this I've picked up from experience and having conversations with people in the business about the controls that's been put in place at Engen.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

Yes, I think that the Engen information, the news, I think we try to use as much as we can when it comes on the Internet. Put posters up. I do think we try and inform people, but people are not always very aware of what's going on.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

So they were informed via the Engen news, but still I think that a lot of people were not aware of the changes that were made, so we would use communications, straight emails, and I think probably being a bit more effective would be handing somebody a piece of paper. So according to me, Engen news just use email as a source of information.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

I do think so. I think it should be, it should work on a first strike. Process more information sharing, explaining, and if it should happen again, I do think that there is no consequence to them, to somebody breaching, even after being informed that wanted done initially was not adhering to the security policies. So I do believe there should be consequences, although the users should be made aware before the time, so I think it should be on a one-strike, two-stroke basis.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

Judging by the amount of breaches we had with the testing on the phishing, I don't think its effective for the users to continue although I think that from Engen's side, we are trying to keep people informed, but it does ultimately fall on the user to actually look at the information, the access given, the information they are given, to actually look at the information and understand it. To a respect, the way I see it, that you can only do so much. You can't force somebody to read an email, you can't force somebody. If they do not understand, they probably won't ask. I do believe we do provide adequate, or I think we do provide adequate information. Forcing people to go through security training is a brilliant idea. I think the constant testing on the phishing campaign, I think it's good. We do keep people up to date with the latest trends most of the time. I think it is falling a bit on the wayside. The relevant topics are given to the people, to actually, I do believe it will provide.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

I think to probably be a bit more visible on the process. I think putting them in the strategic areas, I think brighter posters, and I think posters that are catchier posters that are very pertinent to what's out the world. The emails, I think it might not be enough, so I do believe that having bigger brighter posters, more catchy posters, in the area where the people congregate like the lifts, like the pause areas having more in-your-face type of posters will probably catch people's attention.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

From a technical side I would say that find it is quite good and this comes from the culture between the technical teams working with each other that is good. I think out in the business, I think once again comes from the human aspect, so from a technical side I think this is well. From a personal side I think it could be improved.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

I think to get the people talking, and an example I would say is well, once again comes back to the posters. I think maybe we should use video, very short video. I think maybe little information cards, small little ones, that just in your face information.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

I think a real world situation, things that people are aware of. I don't think talking about a Ukraine breach on the nuclear power plant being pertinent to South Africa. I think more dealing with the more home grown situations. I mean, an example would be the rats we take in our retail environment, nobody knows about it and I don't think people are aware that if it had happened at Engen what the consequences would be. I think using examples that people understand and that is more relevant to their situation.

APPENDIX B2: INTERVIEW ANSWERS OF PARTICIPANT 2

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

Implementing security culture is very difficult purely thinking for Engen because nobody wants their system to be touch on and here at Engen there is silence. People want other people to intervene in their areas but you are in charge of securing the environment but they don't want you to put measures in place because it's going to interrupt their environment be proactive about it so challenges is the slow and protective about their environment. The culture here is one of the most interesting cultures I have ever seen. There is always time to apply something tomorrow, nothing is serious, nothing is urgent, we can also need to.... things that can happen to intruder's intrusions. Yes, they do and yes and no you get the responsive users than you get the red active users and the responsive users, some of them don't and some of them do, so you are there to make sure that things are in place for them to listen like security awareness programmes make it mandatory. So yes, there is some that do listen but here in the security department it is mandatory for us to be the example for the rest of the company and you do get those who do not listen who adhere to policies and they need to be looked at and punish accordingly.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

Yes and no. Yes, because it is out there; we hear about cybercrimes because IS security or cyber security been made aware of the *Wanna cry* outburst on... the user awareness people knows about it and that also know that people is just at ease and they are under the impression that this will never happen to us.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

Not fully aware, they don't think they know the full extent of what intrusion can have on a company. Me, being a student studying for Cyber Forensics has come across a few examples of how intrusions has closed company doors and, but still there is people out there that is not aware of the full extent of how this can impact a company.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No, this is purely because I'm speaking from a human point of view. Humans tend to pass the buck or not take responsibility if something goes wrong, they then in retrospect, they tend to want glory or fame when things go right. So I don't think they want to take responsibility for it but somebody needs to answer at the end of the day. Although the CIO makes the decisions the users should take responsibility for any breaches.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

The biggest challenges, as I have mentioned before, is of the silos that is here. The people protect the environment tremendously. They do not want our departments to scratch out their environment or they are very protective of their environment. Something else I've noticed also is processes – this company is very process-driven and sometimes these processes have an impact on the actual work that needs to be done because processes take time. Because approvals needs to be done, it goes through a whole long list of approvals, goes to a whole list of testing, a whole list of everything before the actual work gets done. So processes need to be re-looked at this company through maybe streamline it and make it more effective. For now, that's the only thing.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

Yes they do, I believe they do. There are a process of change at the company and everything goes through the change... so that is also awareness, a security awareness that takes place which every month a

certain person has to make posters and print it and the guys in the mailing department will put it on the lifts or where its visible wherever people have exists and so there is definitely awareness and training. The training I think is, there's is security training that also happened. I think in last year some time and which were mandatory which I think especially with the fraud and acting bribery. There is training that is involved but maybe a little bit more would not hurt anybody.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

Like every company, change is inevitable and change always disrupts employees and there's always a bit of anxiety attached to change and its exact same here when we changed from remedy to service now the there is a whole hype of will this be in there, will that be in there, will it accommodate this. So there will first be complaining about it and then they will make it work but that is notice of how Engen works. They first complain about it but if there is no other way, they will just…

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

Yes. It should be put in your KPI, how many times you breach a certain incident, or a security incident should be put in to reach a certain amount, whatever the case. Maybe then you score a zero or you will score a 3 or 2 of 5 or whatever the case may be because this should be part of your KPI. I believe that people should adhere to it and there should be some punishment attached.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

The thing is, there is no security training now, the security team do not do any training, they do awareness so they make the users aware of the threats but they do not do any training for users as such.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

I would say training is one of the first things. Some security training would be nice, maybe break down the silence, the departmental silence, interact or mixed-up teams that can work together, that's all I can think about.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

The culture is, for me is hardworking, definitely. The culture is of such a load that they are dedicated to protecting the environment of Engen put measures in place, vulnerabilities, and also try and prevent intrusions if it is internal or external. The culture is of such a serious, the work that they do is serious, so please adhere that is the culture that comes from the security team or my…

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

There is a few ways that for the sort of time I've been in the security team I think how current manager is doing a pretty good job keeping the security team together and also the very high profile and very serious position and also very serious area we work in, so always adhere to, although there is moments we have fun but creating a more better culture than we are now, I shall imagine. So like I say, I'm only a year in so I'm still busy learning, in any case, so I cannot add much to that because what I've learned thus far seems right to me and seems that I will use this whatever build up in this year as a building block for culture in a different security team.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

Attitude, that will be the big factor, attitude and honesty. I think attitude in this team plays a big role because you need to work with everybody

in IS, not only IS, but in this whole building if anybody breaches we need to address so we need to have the attitude the right we need to be a people's person, we need to address things firmly, not rudely, but firmly and clearly.

APPENDIX B3: INTERVIEW ANSWERS OF PARTICIPANT 3

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

Engen I think they do try. I think it's a bit too complicated for them to understand, especially for instance say passwords, like when we went from to... passwords with very big long 14 digits characters password they were so confused and they did not know how to put it in... So they do try I think a lot of security confuses them.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

No, I do not think so. I think basically from a business perspective, they don't see the IT part of it because in their eyes it's our responsibility, so it's like this division that's drawn. That's your responsibility and we're business so I think a lot of you know and like to be spoon fed and a lot of it is they don' take that much responsibility.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

I think maybe to a degree they are, because they still try when we implement something, they still try to meet us halfway. Not too convinced on that.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

I do not think so, because I think they still feel it is our responsibility. It is… I think business that can be breached and people start responding. It's like the other day there was a lady that she's from audit and she

just wanted us to bypass all of our security and just give her access from the system and her like your audit you should know that and I'm she was so no I'm like in a rush now so they still fall back onto that business. I went to her desk and I read her folder.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

I think like, you know our world a bit more of a complicated side, but like a very low level maybe integrated with the on boarding, the induction. You know, just have somebody from security start speaking to them, they actually start getting comfortable with the idea of security and you know, like it's there to...not a business us and them..

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

On our side we just see that they... it is not a lot of training from access management side, yes, I think it can be approved on.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

I think basically... email... I think they just feel a bit worried because there were a lot of calls at the helpdesk. The helpdesk tried to calm them down; after about a week it started calming down and they also gave them that soft password tool and... service tool and... copy and paste the password...

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

At least something that you know will help them realise how bad it is. I think there should be something maybe like a warning at liberty we

have warnings. A password actually tests us and cause they would get these guys, consultancy people, in and like you know they did the other day, like that and there were no repercussions from Engen's one but... well they actually gave warnings to people that don't follow the rules. They just phoned us and email anonymously so that was.... It is quite cruel.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

No, I think we actually need more... I think we will know... maybe. No.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

I think that if we can have more visibility of security as if we do not really have anything to do with security maybe you know have like a security awareness week maybe... being in the IT department... you can go around and listen to all the vendors... so you have like a day where you have like different security personnel… keep people... prizes or... people always wants free stuff... always remember the security.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

I don't think we have too much of a security culture, cause everybody, especially where access is concern, they just want access. They don't think there is consequences to what they are asking and it start with management coming down on you to get that... not listening to people problems... We basically try to explain it at first and if they still don't, we escalate it on our side, yes.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

I think maybe if [the CIO] have the training to understand what our processes are then maybe he will be more… before we educate the users we must first educate the managers...

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

You think relying on the wrong tools thinking… maybe like that you know having that day for security awareness and maybe that's another outlook, getting people interested and getting them phoning us. I think their silence actually creates that wall. Nobody's actually interested in 'you will do this and you will do that'. I think it is both, definitely. You want people to engage with you and you want people to be interested in security, otherwise they will never actually use security. The video will be multimedia.

APPENDIX B4: INTERVIEW ANSWERS OF PARTICIPANT 4

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

No, I do not think so. Well my answer is no, well I think if you sent out a survey just about security where you might want to, you know, if it is a malware or even if it is a virus that you send out. If someone actually goes in there and not be aware of let see where its comes from and things like that, so I don't think they really, I won't say they are not aware of it but they don't take note of those... it might not happen too I think that something that probably how you get it installed, I don't know.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

Well I think they do even if we… if flyers were send out, even notes. Some of them because they not forced to read the notes you get a lot of people go 'ag hier is alweer' Engen news, or wherever, they delete it. If there is somehow a way that you can actually force them, you have to open and acknowledge that you have been there, probably make them a little bit more aware instead of just bypassing that.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

Look, I think they are aware of it, a lot of them they will not do anything. If a person can sort of make examples of maybe some users even if it's just a hoax that you send out because you can make some sort of example, you can actually make them more aware of it and they will actually be more vigilant about it. I shouldn't do this at the moment because nothing happens if I do it here I can go to this firm and they can clean up whatever they want to. If you, can you, know put a responsibility more to them, look, as a company you are to be responsible for whatever comes in. Also, make them responsible for...

because there are certain procedures over everything you need to do…

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

I do not think they take ownership of their actions because whatever the information... let us make it somebody else's problem. If I can use an example for argument sake, we've got a lot of, you know, official things on the g-drive... where you have certain people that has own those things and you are comfortable and say… because you want… to me... you know what... You know there are people that kind of know they can't have it because xyz most of them I mean working with access all the time. You go to them and they say, o no I am not really the owner anymore but anyway you can give it… tell me you can rather singing it to somebody... but know it is the owner, this is the lacks. I mean I've been in the access game for quite a while so I know...

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

It's to convince the people that there is a risk out there and I think for as long as it has not happened to them. I think it's the same old thing... any other... this information... you look at this from the outside. If you tell the people, look you must lock up because they can break in, they say, ya but I'm in here so its ok. That's the same approach the people take here as long as it hasn't happened to me yet. I'm ok because I think there is you know secure things... and it's not always that.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

I don't think so. If I can use an example where they put the, you know, the memory stick where they've tried to do... they've implemented and secured it and then a lot of people can ask why you... because and if you tell them why, they say ok. You tell them I won't be able if you don't know because of… you won't be able to get your and yet the people put something in… we need to train the people and tell them if

you don’t know this, there's no way that we can actually get it back to you and I think that on that note we... I think the type of security that we have here is something new and we have not really put a lot of emphasis on that so I think the emphasis on the training and making the users aware of... If anything happens you have lost it... we're just trying to pick the data of.... Engen's data.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

I think I've answered that a little bit earlier on where I, we send out Engen bulletins and not just security changes, but any changes that happens, there's not a lot of people that reads it. I can't tell you how you can influence that kind of people if you can find a different way of maybe either get a flyer on their desk even you can school without the notice… It might struck a... just read what is here because I think the people will more than believing whatever Engen... probably if there's something coming on their desks… Let me just read that. Look I know we've tried to move away from paper-based but for now the paper-based stuff... unless there is a way to enforce them to read a new bulletin that comes out and not just send it to a file somewhere.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

Well, I know there was some action taken against users that visited inappropriate sites. If it keeps on they would, currently we've got some lock down on that there are ways and means. If you know how to get passed it, then can you pass it? Maybe they should just be more vigilant about the user, not only say, look we give you the companies to judge. We have caught somebody out already where they have applied for a post. In the past we gave you a password, nowadays we send it to you and the self-service password that you can change, your password. Obviously, if you do it over the phone, you need to speak to the guys and ask him certain questions just so that you can know it is the guy. You can then give it to him but if you suspicious of it that you can actually stop the guy and say look this is not something... I should give you the password, I mean, I've already have in the past where some people phoned and I know one day a guy phoned me and he said that can we change the password for and it was actually the manager of that guy I knew the guy he phoned and requested a

password change for one of his workers, so I gave it to him and he actually went in to go change the password, so I said to him [name], 'het jy jouself ingelog en die password gechange?' So he said yes. So he asked, 'hoe het jy geweet?' Toe se ek, 'nee ek het jou... gesien'. I've tried to catch him out and then I couldn't keep my laugh... your password is your responsibility.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I don't know, but look, in some cases there are, I know that there are a lot of people that specially if we come to pass... ok they don't always remember the answers to the questions, they will then phone and ask you to reset questions and if you can and they will actually putting in new answers and they will go in and change the password, I know that when they phone the helpdesk, the helpdesk... and then the helpdesk will then log a call to us, to either reset their questions or unlock it… I think there is some degree of effectiveness in there but not as I think Engen would like it to be. I think specifically talking about this is that the SAP password where there is 3 questions that the user needs to answer and all those are the same questions, maybe we should have a set of 5 questions but you have to answer 3 of them correctly because if you answer the 3 wrong the system logs you out, so what you should do, give the guy another 2 options without the system logging them out and then you can alternate the question, the system should be clear enough to pick up if there is a wrong answer... I do not know on the landside but this is from a SAP point of view.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

Well, like I've said, maybe some flyers on the desk even if it is on a monthly basis where you can even in a light-hearted way, even if it is to make them aware that there is we shouldn't do it when something happens or if we want to make a change even if it's there every month we can even have a little competition to give somebody a change. And those are the type of things which users normally responds to so and as a you know as a person who sends out these questions you can see it's the same people coming back with the answers so you should then encourage to say you can't get the same person to win two or three times in a row. Even like when you log on we put your ID in and

you put your password in before it comes up it will ask did you secure your password… because you cannot just go further.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

Look, I think there is some awareness out there, other than what we have but it is not at a point where we can say we are comfortable, so we still need to work on that. We are getting there slowly but I think it is not where Engen wants to be.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

Look like if you want to send an attachment of any information for that matter, it should actually if the system picks up that you are sending out an attachment, then you say are you sure this attachment is going to a secure site or the person who's going to receive it on the other side just so that they can be aware that there is... you would be able to pick up if it's going to an outside person or inside of Engen something like that I don't know if something is at the door but just to make the people aware that there are some steps and how we can see look I know that for an example there was a lot of people that you know do certain things on the h-drive and to them the h-drive is my property and I can't see anything and then they will have like casual conversation I go to them and say, don't store things that you don't want others to see. There are people out who work in Engen who can go look at what you've got on there because they have to browse through the things on there to see if there is no viruses or whatever... and we didn't know that you can see this, so maybe even in terms of that, make it aware to them that they are there Engen who have the capability to look at those things If they suspect that there is anything.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

Look, I think it is more the awareness of people. I, we can make them aware and even put some of the responsibility onto them, then they would like if I… it might be a stupid example, but in the past we had people, they change their password now and then 10 minutes down the line they still forget it. I change my password today and I forgot it. Anyway, you normally pick up, you get the same type of people with

the same people calling for the same thing, and I always say, if we had to charge you people to change your password, Engen would make a lot of money. I think many people will probably be on about it, but that it might even stop them from forgetting their password. The other risk of that is they might still… so you need to took away the... I think the difference now with the bank card that is you can keep the same bank card forever access within Engen generally the password is 30 days and it change now to 90 days, but with that, the more complex it became sometimes making it too complex can be a bit, did I put a question mark there? Did I put a special character somewhere in the password? I think that is probably one of the challenges. Well, I think what some people does when they see complex password I must choose something... and then… look if you can choose a phrase that you can remember with 14 characters it is not that easy. You can use a simple phrase as long as you adhere to whatever you need. Look, what I normally do when I need to change my password, I would just look around in my office and I see the broken chair I would use the broken chair as my password and I know that's a broken chair because I'm going to look at it the way I spell it is for me to know. Something like that.

APPENDIX B5: INTERVIEW ANSWERS OF PARTICIPANT 5

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I would think more no, for example let's take your SAP passwords, so I mean they are now 14 characters, which makes it a bit more tricky, let's take your normal hackers password unless you have your system forcing capital letters, special characters, digits you can say the system is more secure but they don't, then instead of making it something that you will know, something that's not easy to figure out, users have issues with remembering so they would make it one capital letter which is S and then the H and the O for... they make an @ sign something easy like that so I don't really think, so I think they, the users, find ways around it to make it easier for themselves intern exposing the company to...

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

I think they know, the meaning you know you need to safeguard your... you know that's your responsibility to not share it with users. I think yes, they do.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

Not fully. They may be aware but not really worried about it, for example, the sharing of log on details, only that happens so often and it's a risk. I mean it can get into the wrong hands, so something that they know, so they are aware it could be a risk. I don't think really they are aware how real the risk really is.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No, they say why did the system allow me.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

Definitely, as you said, human related. I would say acceptance adoptions, as in I've just said, people needs to accept. Look, there are certain processes in place that has to be followed and adoption has... outside as well like in the users mind set... we not going to moan because now you need to do 3 steps instead of just 1 step whatever we are adopting, a proses, this is what's in place we are doing...

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

Yes, I think so here and at my previous organisation, it is whether the users utilised the training and actually take not of what is said and done, that is another story, but yes, there definitely is training available.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

I have found users are set in their ways and do not like changes, and what's worse is that I've found a lot of the consultants are the same and they are much worse. That's where the changes are supposed to come from so users, non-users... when you make a change.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

Yes, the severity of the actions however depends on the violation or the transgression, for example, the prohibited website. Yes, I was once on the receiving end of that, it was an accident. You Google something and then pops up another screen and it's something x-rayed or whatever this is still on your name they come around you... something like that, definitely multiple-time offenders with things like sharing your passwords and... information. Absolutely, it doesn't help saying, don't do this, you have to take some form of action.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I do not know. I would have to lean towards no.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

I actually think there are too many processes for similar things, so I actually would say instead of creating a process, you should change things and simplify it, to answer your question. I would definitely say the proses that does an awareness crash course type of thing and so on especially support... so this is how Engen works, these are key security points whatever these are... these are you will be locked up so I think that would definitely be something when bringing someone on board to give them not a lot of information, but give them the key parts.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

I think everyone wants to and knows what has to but at Engen things are not taken seriously enough for you as organisation went overboard maybe looking too serious, so I would describe it as could be... things can be taken a little more serious and move a little bit quicker.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

No answer.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

Teamwork, so there is a certain proses in place for security reasons or whatever take, for an example a password reset, prevent things from happening in production or your access in production we for example have access to bathrooms and things like that there is... so what happens is the support, people kind of force it down on the users which is hundreds but when it comes to… passwords is not working... password self-service and then the user was like no could you do it and register the questions later and then the person that they spoke to were... like we need to enforce security there are processes that applies to us as well.

APPENDIX B6: INTERVIEW ANSWERS OF PARTICIPANT 6

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I don't think so if I just take the most basic entry level into our system that's the password and I think our users lack creativity to actually adhere firstly they don't read they don't know what the password requirements are number of characters how many special characters and there are many times where they would say I don't have time for this, their attitudes towards passwords and that is the first entry into our system and you of all people will know that the passwords has to be complex they don't understand that.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

I do not think they understand the full responsibility although I think they are aware of what the implications are, but I think they have 'this will not happen to us' attitude.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

I don't think we have ever made an example of anybody, so I don't think they are aware. We don't have a culture of holding people to Engen's standards or Engen's policies unless it's been a confidential incident that... if someone has breached the Engen policy and actually take action.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

I don't think so, I always constant when I move away from my desk and I always see unattended PC's open that is something very we use to play games where I'll send an email when you leave your machine open I started doing that here than I think people started taking offence of they told me I must not do that so then I use to set at the desk and send an email to the people in your team and invite them.... and then I won't mention names but people got upset people that shouldn't got upset but people in the security teams can't do that...whatever and that and if I were to sit down at your PC and sent an email making you will then know I must leave this machine...so people saw it as something else other than something that helps to create awareness, so my answer is no.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

I do not think they really have the workforce to have somebody that sends documentation or even a one-liner once a week or once a month. We have the facilities to use and to share information, and I don't think that we phantom that into our tasks, and besides, I don't know how people will read it. That's why I say you can't go through a whole article once a week, just a one-liner. Well, I can understand that the people want their emails to be sent.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

I think that the kind of change that is to be done I think where If it's simple change, no we don't inform the users or we don't give them enough information about the changes and only if it's a change of a very important nature then we will, but I don't think we will be so keen on I don't know whether it's a manpower issue or I think that we underestimate our users and personally I think that the way things are going now I don't think you should be a security consultant to understand the... the need for security... so everybody that's got a smart phone a tablet a PC they should kind of if you go on the Internet you should be aware of and especially when it comes to personal information something as personal as simple as a letter...

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

Well if I look at the password complexity there weren't much issues or there weren't serious issues and I think the people adapted quite quickly to that I'm not sure how aware they were of why we did it I'm not sure if it was actually necessary to share with them why we did it I did enjoy the communication that they sent out to the users they once a week they sent out something informing them that password complexity can happen on this day did you know… that type of thing that was actually so that I think and I speak under correction I think that was a project and I think there was a there might have been a project assistant manager's assistant that has the time to send out the communications...

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

We kind of restrict websites and we can't restrict every website but I think when it comes to prohibited websites there should be serious implications if you want to for example go on a website this is not the place for it we are not judging anybody and we must always be mindful that we share this space with other people so just out of respect for your colleagues you need to be mindful of what you are looking at and it has to be appropriate to what's required at work and if you are doing inappropriate surfing than I think serious action should be taken when it comes to the sharing of passwords I think we need to remind people more that there are Engen policies against sharing of passwords and its actually very difficult to manage especially since we have... purpose they basically they work outside...than we work and I don't think that we have sufficient monitoring personnel or tools to alert us to that and I think that the action against people like that shouldn't be as severe as people looking at the...but I think that warnings is appropriate people who transgress their passwords and Engen's password policies.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I don't think so. I think in the new structure, I think that we should perhaps engage with the training department and maybe work on a section in the Engen induction where they go through the Engen

policies and they should actually brief people on what can be expected if you breach. So that person will know that everybody has been communicated to and it's not like you can say, I didn't know. I think there is a definite place for that in the induction and I think we should engage with the training department to have that included.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

Well again communication that is key I think we can do like one liners they call it did you know campaigns where once a month we can say did you know this and that and yes so if you keep the communication lines open you can actually I think the users will understand that there is certain requirements from their side to secure their own work environments and particularly the online environment and there is lots of interesting facts on security breaches people might not go and research themselves but would be keen on finding out so if we are able to share that with them I'm sure there is lots of information so that comes to communication and then I think amongst ourselves, my earlier example is that when I walk around, I don't go walking around on other floors. So when I walk around, I walk around on our floor where we have people in our own team in security minded people that walk away from their PC's and leave it unlocked. There's people in IT that in my opinion they shouldn't be told about security, that should be part of their work culture and they themselves walk away from their PC's leaving it unattended, open, and unattended, and so it's like living by example. That's we as IT must adhere to Engen's policies as an example to other people and I think we should always be aide aware or not made aware there should always be mechanism where we inform them what happens outside learn from other people's mistakes and yes we know there's always workshops that you can attend I don't think we promote that and you find that a handful of people will go and other people won't go so I don't know if people think that they can't go so I think we need to be open with the people the users especially the IT users that you should be able to go and spend a day away from work learning about something in your area and that as a result you come back with things you can share with others.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

Well I think that we do ok in that we familiarised ourselves with all the new technologies and its actually very important and also realise that the new technology is not that we implement a technology and that's the end of security... there is a number of barriers that needs to be... and that it starts with the password and might end with information or technologies and that we should be able to budget for these things. I think this is something that really needs to be driven from the higher levels of management where it's important to them that the message filters down because I don't think I've got the muscle to threaten somebody, and especially somebody in a higher level than me to keep them aware of what's required. So, I think you need to buy in from management and their communication, but I think to know that there is no one solution, that you need multiple barriers to secure the environment.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

Well as if I said that should come from the top, it is a little easier to… American company and they've got a policy called SOX, and SOX say the CEO is responsible and because the CEO is responsible it's in his interest to make sure that everybody adheres to Engen's policies and sometimes have to force a culture, sometimes its easy case its interesting, security is interesting to us but not to everybody, so some things need to be forced, enforced, and other things are not as difficult to enforce because it's interesting. But yes, it has to come from the top and your security consultants have to learn the security, you have to constantly learn, I mean it's an ever changing environment and if you go on to where that its ever changing, we will fall behind. So never fall behind, always keep up date with what's happening out there, use examples in other companies; ensure that we are following the right path and effective communication with our users, with our online users securing our information and that's another thing – I don't think people give information the right amount of importance. You always find that people say that the staff is the most important, staff can be replaced, information can't be replaced. You only have one opportunity to look after the information.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

Well again, it is leading by example, from the top down, living the example and effective communication.

APPENDIX B7: INTERVIEW ANSWERS OF PARTICIPANT 7

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I will say yes and no. When I say yes, you do get those that… they do adhere based on… they do follow whatever they being told, for instance they do read the posters when it is put out there. I'll say no, for an example, some of them they still open things that are suspicious, which they don't know what it is. For me, that's an indication for someone not reading what has been send out there by security and any... that has been made by the security team.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

I will say yes they do, but you will find some of them they choose to ignore it because sometimes it contradicts to what they need to do.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

That could be debatable. Some are aware some are not, they just found a reason not the obey, for instance, some of them I think, for an example, I think them some of them [are] more open for curiosity situation where they want to see, if I do this what's, going to happen, not knowing the consequences of what would happen if they do that.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No they don't because they are always looking for someone to blame, always blaming. Why was this not prevented? Why didn't the security see this beforehand? They are forgetting they are not acknowledging the fact that they are the cause of the problem.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

I would say educating the people that know nothing about security, it becomes the point whereby you are... you took a language they do not understand, so it makes it more difficult for them to understand what we are talking about, how much the debt of the course where security is concern.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

Yes it does. An outgoing email sending out to the whole company alerting the users of the current situation what needs to be done. Following to that, there re posters is located on each and every floor within the company that everybody must read, understand. We try to make it simple enough for them to understand awareness.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

The inner mechanism, I would say they do utilise it. What they do read, how little they take, we have no control over that and the posters as well – they read them. They respond more to emails than posters and then in terms of the posters, I cannot really comment on that because I'm not there when they do read. At as I would say, it is effective, they do read it.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

Yes, action needs to be taken against that person because for starters, you are being told of the risk all the time. It is your prerogative as a person to adhere to that. Have you chosen not to do so, it requires some action to be taken against that person to teach a lesson to that person so that they need to listen to your rules of your security.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I would say yes, it is very much effective.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

At the moment the one that are more effective is the in-house which already been done, but additionally, I don't think in terms of... remember even all the users that are all on the road, they are email collected of which they can mainly access emails so basically they do read emails. We cannot emphasise more that we are actually doing by emails and posters everywhere.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

Yes they do. That is the one thing I have noticed, everyone is the… When it comes to security is very much... around Engen, they take it seriously.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

It's a difficult question because I'll say in terms of like saying... into emails then already the exchange does falter. I would say having to allow users to only receive work-related emails, but that's going to be a

bit difficult at the same time due to the vendors, because they must have a different... and Engen's one that may not be effective.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

Like I said, mostly I would say it's more curiosity because for instance, some of the mail will come via email a person receives and email they want to see what's that, although in the back of their mind they don't know what is that, it looks suspicious but they have the mentality of let me see what's going to happen when I open this. That's what I think in my opinion, that's what they do.

APPENDIX B8: INTERVIEW ANSWERS OF PARTICIPANT 8

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I don't think so. I think... the Engen employees are not educated enough with regards to security; first to what the function is and what it tries to protect us against, and what the risk currently exposes in the environment. So more work needs to be done in that regard because that will build culture in the organisation, and that can be done through various communications, training, etc.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

No I don't think so, I think the only way that one would target those individuals to carry the message across is to bring it back home. How do they operate at home? How do they operate their PC at home? How security mind-set do they apply when they are using computers or IT infrastructure in their private capacity?

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

No, I do not think so. I do not think they understand the concept, the lack of concept, they do not understand the risk exposed to it and how the companies are exposed when they are being breached.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No I don't think they take ownership because I don't think they have a good understanding of what is the aspect of one... outbreak, how the

company's exposed, so for them, lack of understanding impacts the responsibility and who takes ownership for that.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

It starts with budget, I think with budget you can go further by being able to spend money on training, have more phishing attacks done, have more awareness posters, and so forth. There is a lot that's bargained on budget; secondly is to create a culture, is the willingness of the normal IT user to want to engage and to have an understanding of what is IT security about and what we're trying to protect from, and thirdly is the availability of resources, to be able to allocate that time to training concepts, training rooms, and having to participate in training questionnaires, etc.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

No, I think changes… like the firewall change, opening ports, those type of changes. I don't think the training is adequate. I don't think users is educated enough as to what changes is happening, the education of the users, because you can inform them about the following changes the firewalls make, the following changes the web makes, the following changes etc., and all the changes, but if they are not educated and fully understanding what does it change and what does it do for Engen, then obviously that will not salt to them. Then it's no use. I think at this stage we need to move more on education, then on providing information this is what's happening within the eyes...

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

So we've got the changes cab that we use for changes but the cab is isolated to, or only exposed to INS, so all changes happening in that it is the users that are not informed and one can perhaps use a… saying the following changes has been implemented towards email, which

brings in more complexity to the issue is that Engen has requested less Engen news being communicated to the users; the more the news comes out the less people are interested in reading it, so it's just the email and that, so something needs to be worked on communication regards changes.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

In a mature environment, yes, where people are well-educated comes again back to the education and the user awareness that they need to want is almost sign-off that they had read the policy, comply to the policy... available for them to read, but there is no obligation for them to abide to the policy or make them responsible, so the only is for them to sign off on the policy saying, you are now responsible for the following, xyz, including, as I said, sharing of passwords etc. Once that is in place, then you got a structure to fall back on saying, now you are accountable, responsible for managing your own passwords. That action should be taken because then the user is aware of his user roles and responsibilities.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I don't think its ineffective at the moment cause there is a lot of talks about that we've brought along, like password complexity, but I think the... for more effectiveness around it. Yet again, budget spending, if we had unlimited budgets we could have done a lot of training. I think users would be educated, but it is a question around budget.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

Education and awareness again, and to make the user more involved, and to make sure that the user is properly informed of his responsibilities to create a culture is almost a gut feel this is how we operate in the environment, but if the user is unaware of what is security and awareness etc. around that, they will not have that gut

feel. So it's more a question of improve awareness, get the gut feel, then they will know what their roles and responsibilities are.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

I think in the last 2 years it has improved cause I see a lot of people talking about ballpark security. More people have conversation concerning hector hackers, etc. I think there is a greater understanding around and the term hacker has been commercialised. A lot of people have now taken on what is a hack, but obviously the technical behind it understand the concept of hacks. I think it has improved, but I think there is more room for improvement. I would say there is some understanding around what security means to Engen.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

I think one is, many years ago we've had, they called it the induction course, so the induction course is a three day period where all new employees are put into a room and each and every division had a talk around what their division is about. Now, I think it's a great opportunity for people when [name] will go here and I would go and hack his induction with the individual, which is probably half a day to tell on IS. As to focus on security, get them understanding around that; it's at that stage they can sort of, you know, what I've had my induction course. I understand what security is about, I know what my rolls and responsibilities are, sign off that, then move responsibility and accountability to the users.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

There are different phases to it; one is there is an awareness, so the individual is aware and now the question is, how do you get from there to awareness? You put up posters, you send out emails, you can do training, but yet again, it is a question of timing and budget. Do we have the availability of the staff to go through that? What we can do, for example, is compulsory online training, so once in a couple of months one can have a questionnaire that individuals complete in so... of where the gabs are. So, if you have a quick say ten questions and each individual within Engen is required to complete that ten questions,

you can use that questions as almost a statistical base to understand what level of the users are really high aware or is the awareness quite high, or awareness quite low, and also gauge where the gabs are and focus on those gabs, because there is no straight answer. There is no silver bullet; one needs to understand what are the statistics around the level of awareness and where the gabs are and they focus on those gabs.

APPENDIX B9: INTERVIEW ANSWERS OF PARTICIPANT 9

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

No. My reason is that in our company we do not have that awareness. Communications are being communicated when you, when the Internet... online in the company these are the risks... more like you can be hacked and then these are the concerns of being hacked, so like those messages are not being communicated to the users as much as it should be.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

I don't think they know, like the communications through the systems is not that much communicated to the users. As a result, users will just say, ok the company has the anti-virus and stuff like that. If we get hacked then it means the company… unlike when it's been communicated... ok be careful... anything can happen.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

I don't think so even if the messages are being communicated, this doesn't have that weight to the users. We're running a vulnerable situation here where like the hackers are always advancing in, but that message is not communicated to the users.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No, I do not think so.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

Number one is communication. Sometimes you communicate, but the recipients are not really into taking that communications seriously, so I would say communications as well as the willingness from the users; ok let me have that corrected, I do not think people are having that time, everyone are just doing their own thing.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

I will say they try but the problem is the users understand that's the challenge... they try to communicate but also they don't follow up... the users.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

Number one, they do everything and then after everything was done then they... so now the... is not just sent to the users. There is no follow-ups.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

Yes, actions should be taken so that people can be responsible for anything. If the system like gets hacked, whoever is responsible should be taken to book. I think not so long ago there was a communication to say that there is hackers from somewhere, I think they hacked some computers somewhere overseas where in like where the hackers... for us local... pay so much dollars and stuff like that, so I would say the action should be taken against those who are not following the security and compliance.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I think they are not, because what happens is when the security teams come with something of some secret measures, they just send it via the emails to the users, there is no follow up to see if really the people understood what they think was communicated to them.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

Number one, the securities driving the strategy should be communicated to the users. There must be sort of some workshops about how security is going and where the systems is in terms of expose the risks so that once people understand the risks, it's easy for them to make sure that they don't put the system at risk. The security team would just do everything, then after that they communicate via the email whether those people understand what is needed, they communicate it to them, there is no follow up.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

I... everyone is doing what they are doing the company... to do. If you are not in security, you are not worried about this thing, the system, because, and also the security people, they don't communicate much about the system. So as a result, people just think, ok we are working in a system where like the hackers and stuff like that, there is anti-virus and they are taking care of that.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

I would suggest that there should be some kind of... look this is how... the way the... is communicated to people... security should be like this way... people are being aware of everything and then once people are aware of risks it's easier for them to see, so communication, making

sure that what you communicate to the people, people will understand what you communicated.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

People who understand security must come and communicate correctly to people to make sure that that people understand, follow up with them.

APPENDIX B10: INTERVIEW ANSWERS OF PARTICIPANT 10

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I think to start off, one of the things that effecting is how we relay the message, so this is all about communication. So that gab, the message is actually not sort of like put across to the users in a way they actually understand, sort of like the clause and the cause of why they should actually do or carry out decisions or tasks. I would say it's a bit of both. Some users actually adhere but the most cases you have to consciously make a follow up because most of the guys fail to understand the after effects of these breaches or when things go south. I guess the old gap is us as… or me coming from information security background, we tend to be too technical. It's mostly like technical theory not really sure or put across show them like in real life scenarios why this should not be done.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

Most people assume so because you know, when a user or an employee joins a company you normally have messages with log on where they tell you this is under surveillance monitoring, your emails. Users generally tend to think that they can always beat the system or no one is actually watching or no one really cares. It's just messages that I just put out there for monitoring purposes that no one actually tends to see what, actually sees what's happening behind the scenes.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

Yes, they are aware of the repercussions but most, they actually just do not care.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No, users, from my experience and my own opinion, users tend to play the blame game; they always blame it on the IT department or the Security department that, if this was in place... so it is always people pointing fingers to departments in charge.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

I would say we all come from different backgrounds, I think mostly professional backgrounds. You deal with users who moved over from organisations where the securities lack. You deal with users who basically have no technical knowledge, its limited, so when you have those people in the same room who always cause issues because they are saying, where I was previously we had access to anything so why should you lock us down here, we are all adults and the other guys are telling the ones who came who is still trying to figure their way around technology they tend to shy away from moving along with what's happening form a technology prospective.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

Yes we do send out email notifications, weekly email notifications. We do send them just informative emails to advise if there is an outbreak of something and the steps we need to follow, maybe do escalation or what they need to look out for. Us as departments send out these notifications. In the second part, I actually not go on a one-to-one or class-based; mostly we do it via word portals or just go visit the zone or just study through a job commune. I think we need like that whole interaction when we meet up with like weekly or monthly discussions.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

Mechanism can very easily start off with email notifications or screensavers that always relay the message across employees every time they do something, or banners, those are the types of methods that we use when we have new security implementations in the organisation.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

Yes action must be taken against these users because research has proven that most of these breaches or attacks that have happened, like over 50% is inside, it comes from within, so if you don't create that awareness and also you don't punish or take action accordingly, then people are just going to cause like a must tell if in like a bad way to the organisation's reputation or loss of data.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

Well, I would say I've not been here for a very long time, but from what I've gathered I would like to think, I have not seen guys attending or employees going for regular like training usually notifications and once in a while when it's more like reactive, so we need to take a proactive where people are trained well in advance regular meetings.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

We can sort of cover up against where you get emails which say, win a t-shirt or a cap. We should come up with games that revolve around information security, take for instance, you can come up with random email campaigns where specific users actually don't fall victim to those type of... they are rewarded accordingly, like who's been following the right procedures, whose been consistent, like they would be rewarded.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

Based on the work that I have been involved with, take for instance, I mostly get access, users, random users, requesting access to take for instance USB devices we know that one of the... that is used by malicious hackers to get access to environments it looks like these. A high number of requests and from how I see it is as if people do not really see the reason why it has been implemented in the first place, which actually makes me believe that they do not really put that into consideration that this actually is a security risk.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

We can basically come up with or go back to the emails where instead of the competitions where we say come up with the best story, this time around the story revolves around why you ended up being here or what has happened to you. You come up with the worst thing that has happened to you from a security perspective, be it an ATM pin someone actually showed us serving or you are caught being hacked and how you manage to overcome that experience. It sort of like gives other people also an idea of how the different security risks and breaches sort of like where the possible... comes from and inform people... regards to the attachment as used across the board.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

I'm sure start off with the team leaders where each and every week they meet up with their team, they are assigning just tasks. Let’s say for ten, fifteen minutes about security related tasks where they go to a specific slide or scenario just for brain picking and trying to figure out from their colleagues how they will respond to a specific incident or scenario. That way it’s always keeping the employees, they don’t really necessarily need to focus on what they are here to do but also see things from a different brand, sort of like a mind-set, it opens up their way of how they see things in the broader picture.

APPENDIX B11: INTERVIEW ANSWERS OF PARTICIPANT 11

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I think as far as possible and as far as necessary users will adhere to the requirements of the department, especially if they know about it. I do not think they willingly trying to subvert policy to get around it, they might experience frustration. I think where we find issues of users not adhering to requirements, I like to think that the most part is because they are not aware of the requirements, and if I can liberate a bit more on that, that really comes down to building a resilient organisation. It comes down to users' awareness of risk and how responsible they are towards that risk, and I think if they have a better understanding of what that risk is and what the responsibility towards it, then I think it would make a better, It would make adhering to those requirements for the users a bit easier. We do see pockets of great adherence where users are quit security savvy and we see pockets where users just do not have any idea of security, and let's not forget, security is not an easy thing to pie even for people who have security experience. So the challenges are really trying to ask users to understand and apply a very complex area which in according to maybe a document or a policy, and I think that can also lead to them experiencing some difficulty in adhering to those requirements.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*
If yes, why?
If no, why not?
I think users have a vague idea of information security and that the idea only stems from activities outside the organisation, to stanch, I think security coming down I'm talking at what point will a user be engaged to security and most likely with their banks, so that might have been the first touch point they will have, where the banks started forcing to... authentication sectors and OTP. I think since then, the banks have always been leading the charge with the rest of the organisations following. An example of that is that banks already have what they call industry search, which is quit a close community, so as an all-gas company some possible to get involve in financial... That

really goes to show the maturity and their long... and trying to apply security... they probably had the most too lose at the onset of security, more so due to financial impacts. So, I think when it comes to the users in our organisation, I think they are aware of the security, probably not fully aware of all of the requirements and that is indeed the challenge that...

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

I'll say for the most part we have some users which, who are aware, and majority who are aware will probably be an IS. I think the further you move outside of the IS, I have a feeling that they are not aware of system... so they not aware that if they... as an example they plug in a USB stick which has a piece of malware on, they are not aware of the impact that malware can have. That malware is a specific targeted treat that's been delivered to the user to insert it into the infrastructure of the organisation. The potential impact or the systemic risk of that is that it can impact the refinery proses and it can impact a large part of the organisation whether potential risk is at with the reputation is at risk and where financial penalties are incurred and the users are not making that connection, they see security as antivirus on the desktop and I think that's probably where it started and not making the information security risk of a small piece of malware that could be on their memory stick on an email through to large part of the operation proses of Engen... function, so just to sum up, I don't think they are fully aware.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

I have seen where users are very aware of their actions and they act responsibly. I don't think users act irresponsibly and I have mentioned before, I think it definitely comes back to, it's all about information. So even if we take a look outside of security the big battle that IT has always had is to get the users or the owners of the information to be accountable for the information and that they should, and to making sure who has access to it but also make sure that it is used in a diligent way. That is a challenge. I see this challenge even today with IT and the owners of the information taking accountability for it, so we can then extend that to the security aspect I think security is complex; users don't have an understanding. I think they need help understanding the accountability for the information and they definitely

need help in understanding their accountability for security and how the control acts against that information.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

I think it's around probably too old. I think it's around building a resilient organisation and building that resilient communication and you know, you don't build resilience when there is a crisis, so you build resilience before you have the challenges, before it impacts the organisation, and that really comes down to continually engaging with the users, continually communicating with them. Its bringing them on board, so what I've learned especially from, is that as a security team we can't just put out the documents, have some training internally, and expect our users to follow the same path while stakeholders follow the same path when there is a... so over to build that resilience, we have to engage them before the incidence or before the follow-up grade. We have to build that resilience and to... you can only do that really by communicating with the users.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

I think any training needs to have a measurement of compliance, so we can't just deliver training and expecting the user base to consume it and be under the impression or expectation that we have successfully delivered training. So we definitely have to follow up that training with compliance checking, so we provide a number of, we provide various training methods by using common organisational methods which include internet, email we are now using... which is a third party service, especially for phishing attacks. We providing that service as a level of training to it as well. If we do not take compliance checking then it's very difficult for us to actually gauge how we improve on our, how we actually do it. So is our training working? Is it not working? And I think with our tech compliance checking it's going to be very difficult to gauge the level of awareness.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

I touch on the mechanism in the previous question briefly, so the mechanism are, we do face-to-face, we do pending email, internet. We have third party service that has built-in training with it and those services are Mimecast, email hygiene service. There is phishing assessments; those have built training with it. We have, those are predominantly the user facing training that we do, we do not do, as users are more in the organisation, we do not do any training as they come on board. I'm aware that refinery does a certain amount of training, its institutionalised training around safety for users that comes into the refinery area. I am not aware of any extensive security training that... at the moment we see the mechanism of the how common organisational methods are... predominantly email and internet and some third powerbase services which are bundled as part of the service.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

That's not really my feeling and it's more of an organisational mandate. Policies are mandated, so something as a policy, there are certain procedures to be followed, there are your talking to non-compliance to a policy, there are disciplinary processes that must be followed and they should be followed, they should be taken up with HR and the right cause of action should be followed. You know, if there is something in a policy and there is no compliance to it, there has to be an investigation and that investigation will provide more information as to the severity and impact. If we were to put out policies and are not going to be adhered to which we say must be adhered to as a policy as stated, then should not really be a policy, should it? So, if we are not going to enforce it or if it's not going to be any actions taken against users who don't comply other than be moved... the policy is to guide perhaps it was put as a policy... the organisations through time than that limelight needs to be assess for capability, it should still be a policy, it still is a policy, then there should be appropriate action taken or else must be used to guide operational procedure. You should do this which should be a guide or you must do it, no interpretation, you must do it pending investigation.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

Interesting question because I suppose it's how you define training, so Engen does not want to give many training in a classroom, so I can't comment on that case. We are not doing it, I can only comment on the training that we do provide, which is email training. Also we do posters when the impact has been, the probable impact has been quite high... we do have to have additional things, waiting at the turnstiles and providing awareness slips to individuals carrying it. I feel that's been really good, that's been rather good. This is what's happening, this is what you should or should not do and that creates visibility and I do think we should become more on that. I think the training and the email hygiene, which is another one that we do, I think it is effective because it's on the email, if that channelling comes up it is in your face and I believe there is some good on that; the phishing as well, it is also as it happens, its immediate, I believe there's already been training. The problem of sending out emails that we do, I've had one of the individuals who pass surveys in the organisation, this is not security surveys, it's just organisational surveys. The hit trend on surveys is somewhere between 10% and 20%, so all the surveys that's been send out, they are only giving a 10% to 20% response, and if that survey is going out by email, I can then confirm the email we sent out is only hitting 10%, maybe 20%, of the people in the organisation. Whether that is successful without validating, it's difficult to tell. Those are the mechanism we have at our disposal.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

You know, an organisation is based on risk; the risk has two sides, it has a negative side which is what people often associate risk with. It also has a positive side where there is opportunity; opportunity exists in risk especially when an organisation is in crisis. The negative side and the opportunistic side create a culture of security. I think you have to be risk... if your culture is not risk, if your organisation is not risk... It can be really difficult to create a culture that is security aware and you do that through engagement from senior management, and that has to then filter down through the organisation; that has to be done through communications prior to incidents and crisis happening within the organisation. It has to be, it can't be a type of engagement. It has to be continuous engagement with the employees all the way through the process from start to finish, so just to sum up, we have to see the opportunities as well as prevention against the negative side effects of a risk occurring within the organisation. That has to be done through, from the top, not an isolation with engagement of all the stakeholders.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

Describing it, one of oil and gas which you know in the discussion with peers in the industry, there seems to be a certain level of culture that prevails in the oil and gas industry. In large areas of the business there is really risk. They work in refining processes, they work with refineries, and you know, if something goes wrong it has an impact, not only on the financial reputation, it also has an impact on life. And so I think that's where the risk comes in, and people like to be very aware of the risk. I think what is happening now is quite clear. Over the last few years the culture of information security has been one of a lack of awareness. They haven't been aware of it and only now we see the threats globally that are impacting infrastructure, like energy, like oil and gas, or include oil and gas, which is now bringing information security up into the board level. Now that its reach the board level, its actually started to have a wider impact against all stakeholders within the organisation which puts the ones at risk, some risk, or put ones on the individuals to be savvy when it comes to information security, saying that I think the users and the employees and all in the gas environment still need a lot of help and understanding to what information security is or what cyber security is, or all that.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

So culture is based, interesting question, because I think you first set your own pact what is important. You know, I think once you start to unpack that, let's assume the organisational culture are those things which people do repeatedly which they are familiar with, they come in day to day and there are things that are done continuously or are done off the... or are done without thinking too much about it; it's just a way that people act, its [name] that says it's the smell of the place, or someone says you walk into a place, it's the smell of the place, you can almost smell a culture. So ya, how do you do that? How do you get people to become so familiar with it? I really think it is, really its right behaviours, by changing that behaviours, do you want to somehow change behaviour, to change the culture, you want a culture of security and that's difficult. And I think if you can hit on that you can write a few books and you can probably give up your day job and make a lot of money, you know, because I think that's what everyone is striving for. How do you change behaviour and how do you influence behaviour and the culture? Off the top of my head I would say how do you create an information security aware culture? The way I do it is through continuous use of simulation, perhaps my starting point, let's start with

IT, let's get them in a room, all stakeholders, that we can identify would be responsible for enforcing controls and helping to mitigate trends and responding to terms. I would say let's get them in a room and lets continuously have simulation workshops that we... behaviour to one of this is never going to happen to us to wow someone's doing something about this, this it can happen to us and these are types of steps that we need to take in order to mitigate or resolve the... I think that slowly staff should change the thinking and the behaviour of a few individuals. I think one should consult getting that kind of a mention, it starts to spread out. I think it's a lot easier to do with IT folks. I think once you get them to the, once you get into the broader spectrum of the users you will not be able to bring your user base into the simulation workshop to mitigate a security for what you probably will not get the approval from the line management to do that and... I think... is expand those simulation workshops... your... functions silicate you are PC and... because they really have the touch points to all the managers organisations responsible for planning and organising employees and they are probably going to have the best change of influencing behaviour in the organisation. I say start off small, eat that elephant one piece at a time. I don't think if we don't get our immediate stakeholders, our close stakeholders right. I really think going to battle with the MD's who's sitting 500 000 km away who's not in any way involved in IT, I think we should start, but at the momentum behind us our management if we don't get management's involvement, that I thinks it's going to be an uphill battle for the most part from what I have seen, just to speak about management, they do seem to be behind security. I've been on this road for a number of years and the management support we have now is definitely a lot greater. The Board has a lot more visibility, so I think now is an opportune time to take advantage of that.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

Security is complex and we not going to change. There is no point in, I don't think we should be trying to engage the user and explaining what encryption is and how they should encrypt it. I think they not going to understand it, they just going to miss it and we are not going to change the culture at all, you know, so one of those barriers and I think I've said there must be barriers to learning to why users not learning to be more risk adverse, why they're not becoming more resilient, why they are not picking up the memory stick and just plugging it into the machine, why they click on that email attachment. There is a barrier there and I can't for sure say what those barriers are, but they must exist within the organisation. I think we need to identify what those barriers are; there must be barriers to learn to becoming more risk

adverse, becoming more resilient, maybe there is too much hierarchy. Maybe the hierarchy says I must only speak to my line manager, maybe there is not enough cross-pollination of ideas, that's how the organisation learns oil and gas is quite traditional in the sense that it is the hierarchy still exist. Maybe they need to exist because especially in the refinery area people can't just be doing their own things, but there must be opportunity to learn and I think maybe somewhere users need to have the ability to be able to learn about information security. Maybe we don't have those platforms yet where they can, maybe there is not enough self-learning or self-realisation for information security. I think maybe those are some of the contributing factors that are stopping users from recovering or becoming to have more of a security culture or aware security awareness. Let's identify some of the barriers. I think once we can remove some of those barriers, you will probably find there is a willingness to be more conscience because, let's face it, security does not stop when users leave Engen; it extends to their home life as well to their children. We know within security sphere you know our kids been targeted as well by online bullies and that's the thing, if we can engage the users at their level, let them learn at their level, make it real to them, not just about a bottom figure, do this, it's going to improve Engen's reputation. It's probably, there's a disconnect there, so they're receiving a whole lot of facts but they're no able to make sense of those facts because it doesn't hit home for them. So I think we need to remove those barriers so that there is an opportunity for them to make sense of those facts so that they can make meaning of it, so an opportunity for them to learn and I think that will somehow enable a more security aware culture.

APPENDIX B12: INTERVIEW ANSWERS OF PARTICIPANT 12

RQ1: What are the factors affecting the institutionalisation of an information security culture inside a petroleum organisation in the Western Cape?

RSQ 1.1: What are the challenges the organisation is facing when implementing an information security culture?

IQ 1.1.1: *Do you feel the users adhere to the requirements set out by your department?*

If yes, why?
If no, why not?

I would say, and obviously I can't speak for everyone, so I think there are certain people and teams that are a bit more adverse to the point of implementing, or should I say being in sort of an information security culture, but If I had to go with an answer of yes or no, I would go with no. And with a view of I think people still struggle to understand the importance of having good security in place and the impact of if there are issues that occur, because what's happen is it's going to draw the impact between protecting a password and protecting the revenue of a company, because if you have a small or bad required password anyone may be able to access your system or whatever it is they can have access to, personal or confidential information, and that may have a big impact on the company if it gets out, even though there may be security awareness initiatives and stuff done. But I think with all the information coming through to them these days it's hard for people to focus maybe even firstly on those things, and secondly, I think they still struggle to understand the importance of certain things unless it really impacts them personally, such as maybe credit card fraud or something like that.

IQ 1.1.2: *According to you, do you think users know what their responsibility is towards information security?*

If yes, why?
If no, why not?

I think this is a difficult question to answer, so I think it's almost a yes and a no question, because I think they are aware of the fact that they need to be responsible but they don't almost digested and they're not aware of the, they are aware that there are certain things they need to protect, but it's not like it's part of the fabric and I think because some of the things do take a bit of effort to do, such as maybe you have a long password, now you need to remember that long password or certain things or not writing your password down and so on, so I think the fact that you need to put effort into certain things maybe makes them act less responsible. So I think in most part and I'm talking about Engen at the moment now. I think from an Engen prospective people

are gently aware of the fact that they need to protect certain... of security; however, I think it stops at certain parts of security, so maybe they are weak; they need to protect their passwords. But I have seen someone who has maybe left his bag outside the toilet and he's got his laptop in there, anyone could have taken it an walked away, so I think the emphasis are maybe in certain areas of security and maybe not in other areas, such as maybe even paper-based information, so that maybe from an Engen context, from an general context, I would say people are not aware of the responsibility with regards to information security and data protection and so on. They are not familiar with the responsibility and importantly, it's not really being aware of their responsibility but consequences what they're actually responsible for in terms of what they are carrying with them. So I would say generally it's not the case and I've obviously consulted at many organisations where some teams may be more conservative like the security team, but then you have your car boys who don't actually care about things.

IQ 1.1.3: *According to you, do you feel users are aware of the risk of not following the information security procedures?*

If yes, why?
If no, why not?

I would want to say there are some users that are maybe aware of the elements of it, but they are not aware overall. So my answer would be no, they are not aware of the risk and the impact obviously of consequences of something happening I would say they are not cognitively aware, so if that makes sense of the potential risk of doing certain things and I think that's why they are still doing certain things.

IQ 1.1.4: *According to you, do you feel users take ownership of the outcomes of their information security decisions and actions?*

If yes, why?
If no, why not?

No, I think ownership especially you need to take the example of generic accounts, you can't pinpoint who's doing what and so forth. I think especially in that, and I know that, maybe a bit more exceptional, but I think in those instances people sometimes do what they want to do and they kind of like when pinpointing comes back, it's difficult to know who it was in the first place from and accountability prospective. So I personally don't think so.

IQ 1.1.5: *What are the greatest challenges with instituting an information security culture at Engen?*

If yes, why?
If no, why not?

Definitely resistance to change. I think people especially at Engen, some of them have been in there jobs for 20, 30 years and I'm not only referring to them because there's people that's been here for 2, or 3 years also, but I think historically our organisation has done things a certain way now and I have personal experience of this where you come in and try to implement new measures or sharing information to improve things and you kind of detour a big wall, because firstly, there is no buying in from top management. When I say top management, I'm talking senior management, which is below your CIOs. The CIO may be on-board but below CIO, so I think if your senior managers are not on-board with the importance of security, it's very difficult to go forth and actually implement what you need to implement. The second one is people because they are used to certain things. I know it kind of leans to the first one, but some stuff requires more effort, so if I look at people saying, ok they are not going to use USB's as a personal choice because maybe they might bring in Malware or whatever or they might lose data on it, I mean it makes sense now they need to use OneDrive or whatever. I think sometimes with regards to certain things our organisation has a lot of processes and a lot of governance around things. Now we are going in and there are very important controls and things people are required to do, additional stuff, so they kind of because they are, now they already tied down with the amount of work that they are doing, they now need to do additional stuff and I think a challenge that Engen may have is that we govern with regards to certain things. What should actually happens is someone should actually review the processes and controls and say you know what to do, because remember this has built up over the past 30, 40 years. Do we still need to use the controls that we were using 30 years ago? And now we are bringing in new things, so to make the organisation more efficient and effective you kind of want not just bring in things, but bring things and so value to what you bring in and then I think certain things... So there is no doubt, but it's a problem because if you want to create a culture you need to do information security awareness. You need people to be on-board. You want to have sessions. So budget is a major factor. I think also people at management level don't understand the importance of certain things. I think to some degree also the higher levels above that maybe at the GM level and so on also, because maybe haven't been informed and educated yet about how important it is and understandably if someone is the business manager they are specialised in their area, they might not know information security. So I think firstly, there is bringing together, and education, the cost of educating everyone in the organisation, that's number 1. And secondly, also making sure that you are educating the right people who are in the decision making areas to be able to say you know what I need to give 500 000 towards that so that they can actually make the decisions.

RSQ 1.2: What mechanism is used when making any new security changes inside the environment and what is the response of employees towards this?

IQ 1.2.1: *According to you, does your department provide adequate information security training to your users to inform them during changes?*

If yes, why?
If no, why not?

I don't think they are providing adequate training now. I think they maybe do provide a level awareness through communications but I don't think they provide adequate training around security measures and so on, even bringing in new policies around on how you must do things and maybe if you got mobile devices you need to put security settings or whatever on there. I think we should be having things like training on mobile devices, for example, we are able to access our Engen emails on our mobile devices right through the Internet and webmail now you download an attachment from the email onto your phone, your personal device that does not always have security measures in place – doesn't actually know how to deal with that. My answer would be no, they don't know how to deal with it. Why? Because they might be aware that there is a policy. Firstly I, don't think the policy people are fully aware of, example a mobile computing policy, and this is only an example of this, and secondly, if they are aware of this, whether they understand the importance of implementing some of those things on their personal devices, so that's probably an example.

IQ 1.2.2: *According to you, what mechanism is used when making any new security changes in the organisation and how do the employees respond to this?*

If yes, why?
If no, why not?

I think we need to implement a 14-character password and so on, so I think from our side normally we just send a communication to say we need to implement a password, then we go through our normal change proses and implement a password and so on, and this communication that is sent obviously about it, but I don't think its adequate understanding that goes with that, adequate information that goes with say many times people will just say that's an audit requirement, it's not just an audit requirement, it's the level of risk and impact and consequences that's related to it. I think people are very quick to want to implement things and yes, they do communicate about it, but I think the education aspect is lacking and that's for many reasons. There are teams that's really under pressure, there's cost involved in certain things, but I think there needs to be some sort of thing where we actually communicate the importance of certain things when implementing because I had discussions before people are

complaining about 14-character passwords, but when you explain to them the importance of it and the fact that this password while it's so long and irritating to remember it, the reality is that that password allows us to be more secure and allows people not to be able to enter our systems maybe as quickly as having a very short password.

IQ 1.2.3: *Do you feel action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information or visit a prohibited website)?*

If yes, why?
If no, why not?

I think it's a very difficult question. It's a simple question to ask because I would first start off to say are we making users fully aware of the policies – that's number one and not just policy, and number 2, are we making them aware of what their responsibility is in relation to the policy because I personally found that policies are given and uploaded and approved but very few emails go out about policies unless it's like a new policy. I'm talking specifically security policies. I've had discussions with managers who manage those applications and they are fully responsible for it and they are not accountable for consequences for thing that they may not be aware of… previous application owner two years ago, but a good example is the restructuring that happens in our organisation, who's going and telling them you need to be aware of these 10 policies because you are managing it and an application owner and you need to make sure that your systems are biding and that your staff is abiding by that policy. There is a big element, before they need to be held and consequence management and all that than if you had done that and you done it substantially and effectively over a period of time, then we go to a point where we say the education is done, now you know what now guys. We will have some level of consequence management for the fact that people are abiding by policies. Some policies are quite straight forward. Annually you stay away from work, I would probably ask most employees, they will be fully aware you need to put in a leave request first. Are people aware of information security policy? Are they aware of all of those things? I think to some degree, but I think to a degree not. And I mean, to have consequences and consequence management, you need to be able to hold them to something and if they can prove that this is communicated to them, then it becomes a legal matter and all of those things. So I think there is a range of stuff, but bottom line is, in future when this thing is more solidified and all of those things, then we can kind off move to a thing of that, because, and a good example would be you look at safety when people look at zeta rules and all those things. We need to get to that point and not to the point where someone does something and gets fired straight away, but I think either a warning or maybe some sort of development around their perks and send them for additional training if they are not abiding

by policies. Remember, people are working in very high pressure environments, now they give them a phishing email and you are busy in between a 100 purchase orders, now you click on it, says something the person half look at the email and they click on that link, now they get into trouble. I think there is a balance between the two and specifically depending on the issue that happened to them, there needs to be some level of consequence management. However, if people are doing it maliciously and you can see this is the issue, then that consequence manager should be more immediate.

IQ 1.2.4: *Do you feel Engen's current security awareness training is effective?*

If yes, why?
If no, why not?

I know that there have been emails sent out. The truth is, half of the emails probably are being capped. I found actually the posters a bit more effective only because I go to the coffee area, some people never go to the coffee area. Overall answer, no. The reason I say that is because when I have been having lots of conversations with people, managers to juniors to whoever, there is so much resistance because so many of them has no idea about the importance of security and these are the people who's been in the organisation for 5, 10, 15, 20 years and still they are concerned about why we are doing certain changes or why we are not allowing certain things. A good example is the USB port, I actually had a discussion with someone the other day at one of the… and they were complaining about the USB ports, people not being allowed to use it, but I explained to them what an issue this is and how much it puts Engen at risk. It's funny, they actually seem to get it and I'm not saying that I'm effective but it's just I think once you sit down and have more effective communications, my answer would be that the security awareness training is not effective at Engen.

RSQ 1.3: What processes can be created inside the organisation to institutionalise a culture of security?

IQ 1.3.1: *According to you, what processes can be created inside the organisation to institutionalise a culture of security?*

If yes, why?
If no, why not?

Number one, I think the organisation board from top down, when we did officially phishing exercises, board members, one of the high level board members that was actually in the phishing emails, so they responded to the emails. Basically what I'm saying is, even if you have 30 years' experience or you 5 year old, you can be caught by these things, right. So, number one, board needs to be on board with cyber security. I'm aware that it is a board agenda item, so it is discussed.

The question is, what goes forth from right there, right, and are the mechanism that comes down from the board all the way through the heads of the areas such as the general managers, are they effective and do they understand all of those things? Personally, I don't think that our general managers are fully clued up on information security and what they need to do in their areas in relation to information security, and I understand that because they have a business to run, we have not actually done a lot of training directly with them, maybe come to them... So basically, top down, I know the CIO is actually presenting at the board, so they are generally aware, but the question is, how are they aware in relation to the organisation? So when you keep buying from the top management, which is the board, then you get the GM buying, then you get the elderly level buying, which is your senior managers, then all the way from there go through because when I have conversation with people in… level in the business they are financing perks and all of these things, but when it comes to managing even service providers from a security prospective they have absolutely no knowledge. Number two, our security teams needs a bit of a revamp in their thinking and approach in how they do things because I go to different areas of the organisation and there's parts of the organisation where we don't oversee, but at the same time also we are group security, there is no other security team in the whole of Engen group, surely we should be spending time with them, at least educating them on certain things and roaming up certain things. I'm not saying we must implement controls – that is a separate scenario, but surely like for instance what I'm doing now sitting with them explaining to them the importance of information security and all of those things, so basically we should stop with this thing of it's not our responsibility. We should look at the wider picture, look at and I think there is a level of knowledge that's lacking from a business impact prospective. I say yes, people know and understand the systems and security measures, for example, if we have and issue on fuel facts, how does it impact the business? Are they able to deliver fuel? How does it impact our customers? How does it impact the bottom line? So, I think there is and it also stems from the silos that we have had because people have worked in certain areas, so the understanding of the business is, when I say business I'm not talking of IT technology areas, I'm talking purely business, is from some degree there, but I think based on my discussion that I've had with people, that's been here for a long time in IT. It does not seem like there is a full understanding of what's happening, so basically go away from the view of this is not my responsibility, what is the actual risk to Engen, and how can we try to protect ourselves, even if it's having a conversation with the head of that particular area and say this is important, put it on your agenda, find a way to address it, as simple as that. So I think those two things, I think, from a bottom-up approach, I think maybe we should be having more effective training programmes. So I know at one or two previous organisations I was at, they obviously have this thing called popcorn

training, but you see the thing that I found that's the most effective is when you go through this popcorn training, but you explain to the people the impact of all of these things, you give them, give them very good examples how the one employee lost a backup tape which was unencrypted which resulted in that company getting fined 20 million dollars or rand which then resulted in in that company going through restructuring because of the fact that, but I'm just saying the point is, eventually they can see how this consequences comes back to them and to the people in the organisation and the business overall. So I think from bottom-up there's definitely a major requirement for proper training and we are not saying we need to call 5 people in a room; we can get a conference room we can do a level of training, but it must be once a quarter, it must at least be quarterly, so people come for a half an hour session, we share this with them, but bottom line is you need to keep on pushing and sharing the message from a bottom perspective and from a top perspective, including those heads of departments and their senior managers because I found when the senior managers are on board their teams seem to fall more inline. Because remember I have first-hand experience on this where people are wanting to implement things from a security perspective but their managers don't have really a proper knowledge of security and so on, so they don't understand the importance of it, so they kind of don't prioritised it and they prioritised projects understandably because they are in operations, but at the end of the day some of these start lacking now.

IQ 1.3.2: *How would you describe the information security culture at Engen?*

If yes, why?
If no, why not?

If I should go for rating from 1-5, I would give it maybe a 1, so basically people are still using generic user names and passwords and similar passwords. The unfortunate thing that I've heard and experience is that some of our senior managers that are just not interested unfortunately whenever these topics come up I had people shouting with me in meetings even before they heard what the message was what we actually wanted to bring. So I think I don't know if that is based on history and probably is because its culture and history that comes together, so when we come in with certain things to explain things to people and so on, its already even before they get to the meeting there's this big thing up and negative things on security, more work and more issues, and whatever, but reality I think that perception needs to obviously change. Keeping in mind if you go to the security team they are going to have a high level of security competency and culture and I'm talking about everyone probably outside of the security team, so I would say the culture is low from an information security perspective. I think also the fact that there hasn't been funding in certain initiatives around security awareness and training and all of those things kind of

send a message to say it's important. If management is not making funding available for certain things when some things are not highly effective and it's important, then it rather sends the wrong message. I think also in regards to people who are kind of in needed team leader areas, there's always been a negative view of security and I think that perspective needs to change. Basically there is a very negative view of security when people complain about security and I find there are the odd people that come to me and say you know what, this is a longer password or this is a longer thing, more effort, but you know what, at the end of the day it's protecting us. I think also at the same time I understand that the security team is really quite good at what they do. They do stand up to people, but I think we should try to take a different approach maybe, so maybe we should try to take basically the current approach at in terms or changing culture is not the best approach. Remember, a lot of stuff that we are doing on security culture and awareness is dictated a lot on budgets, it's dictated by time, because it needs to be approved by management. So the thing is at the end of the day it comes down to management prioritisation of all of these things and at this point in time, driving a security culture is not a priority for a lot of managers, but what's important is that since about December, January to now there has been a soft in the culture. The thing is, a lot of these things are quit important points to highlight but importantly also I see more people coming on board cause now they see events happening at other organisations, but the difference is they are now aware of the impact of this, they don't do these things, so we need to get other people in the rest of the organisation, even in IS, to a level of understanding where they are aware of the culture and all of those things.

IQ 1.3.3: *Please indicate and give examples of how information security culture can be created in your organisation.*

If yes, why?
If no, why not?

Firstly, educate management, formal straight up sessions explaining to them, and I'm talking about your GM and don't get me wrong, there are a lot of them that do understand the aspects of cyber security. Maybe some people know it's important, but they don't know what to do, so having sessions with your GM's your... and maybe their managers, explain to them what cyber security is, but importantly what their responsibilities are in relation to cyber security. I think that is very important, and what their teams' responsibilities are in relation to cyber security and what the scope for cyber security is because people think it's just someone clinging to a system. They don't realise that even in compasses and back-up and recovery and even to some degree paper base information etc. I think that's the first one. The second one is we need to drive more better funded initiatives around security awareness to the degree where I mean, I know, when the one organisation did the

exercise they actually ended up getting into the building via the fact that they had a familiar face and they end up getting an entry card, so I think all of those aspects. We also need to address the most critical areas and then, so even like, if someone comes into the building and they don't have a recognised face, they are not authenticated from a perspective of working here, and all of those things. So drive the culture around people, processes, technology from a security perspective. You don't have to have everyone in a room and take up everyone's time, but short straight out effective videos which, the right education, keeping in mind the level and the current culture that we're in, cause also we are going through a level of restructuring. So at the same time people may not be as cognisant and focused as they would normally be, so in these sort of scenarios people might even be a little more careless or loose things more or do things they might not normally do.

IQ 1.3.4: *What do you consider being the main contributory factors to create an effective information security culture at Engen?*

If yes, why?
If no, why not?

I think its people's education and awareness of the importance of security and the impact thereof. I was going to say change, but the resistance to change is any times because of the fact of who caused it, because they don't actually understand the importance of things. So when someone is sitting at the depot and they need to process something on an application, are they aware that if they do something wrong on that application that they could actually be fired when it looks like they causing fraud or whatever case people might do legitimate mistakes, and this is why it’s so important even when someone has access to systems that they know what they doing, because you can actually create a massive issue, even business disruption, and all of those things. So I think the most important thing is the education, effective education and awareness, to the right role players starting from the top.

APPENDIX C: LETTER OF CONSENT

With us you are Number One | ENGEN

Date: 11 October 2016

I **Peter Du Plooy**, in my capacity as **Chief Information Officer** at **Engen** give consent in principle to allow **Michael Michiel**, a student at the Cape Peninsula University of Technology, to collect data in this company as part of his MTech: Information Technology research. The student has explained to me the nature of his research and the nature of the data to be collected. This consent in no way commits any individual staff member to participate in the research, and it is expected that the student will get explicit consent from any participants. I reserve the right to withdraw this permission at some future time.

In addition, the company's name may not be used as indicated below. (Tick as appropriate).

	Thesis	Conference paper	Journal article	Research poster
Yes				
No	✓	✓	✓	✓

Peter du Plooy **11 October 2016**

APPENDIX D: EMAIL TO PARTICIPANTS

From: Michael Michiel
Sent: 20 October 2017 10:57
To: FS-IS ISRM: Security Management <FS-ISISRMSecurityManagement@engenoil.com>; FS-IS ISRM Compliance & DR <FS-ISISRMCompliance&DR@engenoil.com>; FS-IS ISRM: Access Management <FS-ISISRMAccessManagement@engenoil.com>
Cc: Lindiwe Mtsotso (Contractor) <Lindiwe.Mtsotso@engenoil.com>; Trevor Murimba (Contractor) <Trevor.Murimba@engenoil.com>; Gordon Allan (Contractor) <Gordon.Allan@engenoil.com>; Imtiaz Moola <Imtiaz.Moola@engenoil.com>
Subject: CPUT Research Interviews

Hi Team

I am busy writing a Master thesis on creating a security culture inside of an organisation. As part of my thesis I need to interview some work colleagues to collect my data.
Thus, I selected our team to conduct the interviews with. During the interview process I will ask you a set of questions, these interviews will be recorded as I need to transcribe them to word.

See attach CIO consent letter to conduct the research and my thesis thus far. I will setup 30 minute meetings next week with everybody.

I thank you for your cooperation during the process.

Regards
Michael

Michael Michiel
Security Specialist
Information Technology Department | Finance Division
PO Box 35 • Cape Town • 8000 • Fax:+27 21 403 5999
Tel: +27 21 403 4189 Cell: +27 73 727 9283
Michael.Michiel@engenoil.com