1 # Title page

2 **Names of the authors:**

Maureen van den Bergh

Kennedy Njenga;

Paul Benjamin Lowry;

3 **Title:**

Exigencies of Crisis in Situations of Computer Failure: Influence on Information Security Behaviour

4 **Affiliation(s) and address(es) of the author(s):**

University of Johannesburg, maureenvdb@uj.ac.za

University of Johannesburg, knjenga@uj.ac.za;

Virginia Tech, paul.lowry.phd@gmail.com;

5 **E-mail address of the corresponding author:**

maureenvdb@uj.ac.za

Exigencies of Crisis in Situations of Computer Failure: Influence on Information Security Behaviour

Abstract

In the technology-people-management chain, people are predominantly identified as the weakest link in properly securing information systems. An examination of information security literature indicated that the exigencies (or demands and pressures) of computer system failure situations had not been explored as an external factor in influencing information security behaviour. The focus of this study was on how the exigencies of computer system failure situations would influence employee information security behaviour. Qualitative text data were analysed in two phases, firstly, through methods and procedures of phenomenological analysis formulated by Moustakas, and secondly, via a summative analysis. Aggregate results showed the demands and pressures placed on employees during computer system failure situations have an important effect on their information security behaviour, which were influenced towards intentional, non-malicious behaviour. Although no one single solution and/or approach will succeed to fully explain the intricacy of employee information security (ISec) behaviour, results from the current study significantly improved our understanding of how the exigencies of computer system failure situations, an external factor, influence employee information security behaviour. It also provided practitioners empirical implications on how to improve the governance of the human factor of the technology-people-management chain.

Keywords: Information security (ISec), information security policies (ISPs), phenomenology, computer system failures, exigencies of crisis

1. Introduction

Information security (ISec) has long been a concern to organizations and researchers information security managers (D'Arcy et al. 2009; Guo et al. 2011; Johnston et al. 2015; Loch et al. 1992). Over time, with increased globalization, market complexity, and technological advances, organization security has become an even greater concern to organizations and researchers. A key reason for this escalating problem is people. Although ISec involves technology, people and management (Gonzalez & Sawicka 2002; Mishra & Dhillon 2006), it is the threat that comes from people, especially those inside an organization, that can be most concerning from an organizational security standpoint (Siponen & Willison 2009; Son 2011; Vance et al. 2012). This is because employees are perceived as internal threats to organisation's security and predominantly identified by literature as the weakest links in the security chain (Guo et al. 2011; Schneier 2000). The Ponemon Institute (2017) reports, second to malware threats, the percentage of data breaches caused by employees is as high as 30%. The consequences of employee ISec behaviour to finances as well as loss of reputation is well established (Safa & Ismail 2013).

It is in this regard that a growing interest and body of research on ISec behaviour has consequently developed (D'Arcy et al. 2009; Guo 2013; Herath & Rao 2009; Hu et al. 2011; Ifinedo 2012; Siponen & Vance 2010). Adding to this body of research work regarding behaviour, is the role exigencies of situations play (Bamberger 2008; Hong et al. 2014; Johns 2006). This body of work has yet to permeate ISec behaviour studies and this is important because there is reason to believe that exigencies of situations, may have a role to play in ISec studies. Exigencies also underscore work pressure created by a situation and predicate stressful demands to employees (Merriam-Webster.com 2020).

We therefor explore exigencies, by examining situations that bring to bear interesting ISec behaviour. We specifically focus on exigencies in computer failure on either the software, hardware, or networks, which establish grounds for crisis management and stressful demands to employees. As computing technology becomes multifaceted and interconnected, technological failures have become unavoidable (Coombs 1999; Lerbinger 1997). Through understanding the resultant crisis, we predicate a focus on exigencies on employees' ISec behaviour (Bryson 2004). In this work, we present exigencies as a

phenomenon that exerts unforeseen demands and pressures on employees during computer system failure situations, as an underexplored domain in ISec behaviour studies. A central contribution to ISec studies on behaviour, is that this work addresses the importance on the role of the situation (Bamberger 2008; Hong et al. 2014; Johns 2006). The work therefor engages with the phenomenon of *situational exigencies* in detail because ISec researchers need to better understand situations that shape behaviour, as well as explain how behaviour would influence policy violations (Van den Bergh & Njenga 2016). We draw on studies from the psychology domain that are focused on situations more deeply, which consider behaviour to be shaped mainly by the exigencies and dynamics of a particular situation and that people act differently depending on the situation (Mischel 1968; Mischel & Shoda 1995). We envisage that insights from this study can help ISec researchers learn, as well as design, useful interventions that could encourage positive behaviour. Drawing from psychology and understanding *psychological situationism*, ISec researchers can then meaningfully contribute to the person-situation debate regarding whether it is the person (internal) or the situation (external) that is more influential in determining behaviour. We do so by addressing the following:

a) Presenting insights into the situation and how exigencies determine and shape ISec behaviour from real experiences (Mischel 1968);
b) Not only focusing on behaviour, but importantly addressing situational exigencies that can accommodate a useful framework that can ameliorate negative ISec behaviour (Andress 2014; Safa et al. 2015).

Drawing therefore on *psychological situationism*, we apply a phenomenological design in a novel way towards investigating exigencies of computer systems failure. A discourse regarding captured employees' accounts of their experiences of computer system failure situations is presented. Importantly also, the exigencies of these situations and employees' explanations of their behaviour in response to these situations, is provided through a tested scientific approach guided by phenomenological studies. By carefully following the phenomenology design, a considerable degree of interaction between the

researchers as well as the person, groups or situations being examined is provided (Reiners 2012). The sections that follow examine situations and exigencies in detail.

2. Background on Computer Failure as an Organizational Security Threat

Before continuing with our approach to phenomenology based in situations and exigencies, it is vital to review and explain why computer failures represent a serious organizational security threat.

2.1. Definition and Examples of Computer Failure

Computer system failure situations as a diverse set of hardware, software, and network failure situations.

2.2. The Link between Computer Failure and Organizational Security Threats

While it would seem that millions of computers and software programs typically work well daily, it remains essential that we understand computer risks and reasons for computer failures. Indeed it is important to consider questions such as, what would be the acceptable risk, when failure occurs or how do we differentiate between risk trade-offs that may create failure do to perhaps carelessness, incompetence, or dishonesty. There is indeed an important link between security threats and computer failure when these considerations are highlighted.

2.3. Information Security Policies (ISPs) to Help Prevent Security Threats

Hu et al. (2011) define an ISP violation as “any act by an employee using computers that is against the established rules and policies of an organisation for personal gains”. Although researchers agree that ISPs exist to address Information security threats from employees (Pfleeger and Caputo, 2012, Whitman and Mattord, 2012, Siponen et al., 2009), others state that employees unfortunately do not always obey these policies, which is a common problem in organisations (Warkentin and Willison, 2009). The significant number of Information security incidents, as reported by Privacyrights.org (2005) and Privacyrights.org (2006), plus field surveys from Gordon et al. (2006) and CERT/CC Statistics (2004), indicate high levels of non-compliance with ISPs. Just having an ISP in place, even one that is well-defined and in great detail, is no assurance of security (Von Solms and Von Solms, 2004, Mishra and Dhillon, 2006, Besnard and

Arief, 2004). If employees are reluctant to follow security policies because they view them, firstly, as an inconvenience when performing their daily tasks, and secondly, as general directions rather than steadfast rules, then an organisation's ISP efforts are futile (Herath and Rao, 2009b, Stanton et al., 2005, Gupta and Zhdanov, 2006). Strictly speaking, the ineffectiveness of ISPs result in organisations' ineffectiveness in influencing employee security behaviour towards compliance (Höne and Eloff, 2002b).

The importance of ISPs lies in their use as tools to safeguard the use of information, related assets, and infrastructures (Son, 2011). The ISP not only stipulates what employees should do, but also what they should not do, and what the consequences will be if the policy is violated (Baskerville and Siponen, 2002). Often, the ISP is used to direct employee Information security behaviour towards the correct use of passwords and computer system resources that cannot be addressed by technology alone (Herath and Rao, 2009a). The ultimate aim is to control employees' Information security behaviour and to influence them towards compliance (Mishra and Dhillon, 2006). Usually, accompanying policies are standards, practices, procedures and guidelines that respectively proclaim 'what must be done' and 'how to comply' (Whitman and Mattord, 2012).

3. Background on Situations and Exigencies

Fundamentally Information Systems security is established as having a behavioural root (Workman & Gathegi 2007) and as noted previously, ISec behaviour of employees may hinder information security efforts of organisations (Thomson & von Solms 2006).

3.1. Situationism

In psychology, Situationism is a grand theory that emphasises the significance of external factors and situational features that present a specific behaviour. Situationists accept the fact that the present situation is the most influential in generating specific behaviour (Bowers 1973; Candace 2009; Dean 2007). Social psychology's raison d'être is the concept that situations and accompanying characteristics play a fundamental role in shaping human behaviour (Baumeister & Tice 1985; Edwards & Templeton 2005; Meyer 2015). The Situationist position queries the predictive power of personality in determining

behaviour (Bowers 1973). According to Mischel (1968), when people find themselves in different situations, they act differently (Mischel 1968). Mischel continually emphasises that behaviour is formed by the exigencies of that situation, rather than internal traits or motivations and that the behaviour is temporary and based on the current situation in which the persons finds themselves.

3.2. Crisis situations

In general, a crisis is a situation which happens suddenly, that is unexpected, unwanted and in need of some action. As an event, the negative influence on normal operations is high. Action and appropriate behaviour are often required that is over and above the normal day-to-day decision making. Unavoidably, for employees this can cause emotional stress (Huddleston & Pullum 2002; Lerbinger 1997) and employees may see such a situation as a crisis. When employees regard a situation as a crisis, they will respond accordingly (Bryson 2004). Whereas crises are unpredictable, they are not unexpected. Organisations may have frameworks for crisis management, which contemplate the possibility of the occurrence of a crisis and plan accordingly (Barton 2001; Lerbinger 1997).

3.3. Why understanding Computer System Failure Situations and the Person-Situation Debate is important

Our review of literature establishes that situations can influence behaviours in unpredictable ways. What is limiting in ISec literature, is the need to understand computer failure situations as exigencies perceived by employees as crises that interrupt or prevent them from performing their everyday tasks. What is limiting in this literature and which can be complemented from personality psychology studies in the understanding of the person-situation phenomenon, which can serve as important considerations for understanding situations in ISec. The person-situation debate discourse is therefore important in ISec studies, regarding whether it was the person (internal) or the situation (external) that was more influential in predicting behaviour. During the early part of the 20th century, the prevailing discourse was that personality traits were the best way to understand social behaviour (Nisbett 1980). Later, discourse was to place the situation as critical to understanding behaviour (Kenrick & Funder 1988). Studies that have used personality scores in an attempt to predict individual behaviour, found that there was only some conformity

to be found in individuals' behaviour in different situations (Mischel 1968). Individuals consistently acted similarly in different situations only 9% of the time, meaning that personality tests could not explain 91% of individuals' behaviour in different situations (Dean 2007). Following on this debate, is different computer failure situations may yield different ISec behaviour. Interestingly both the situation and behaviour may then be difficult to predict. This is because of the importance of understanding the essence of what it means to be an individual (Mischel 1968).

In studies such as 'what makes good people do bad things?' Zimbardo (2007) emphasizes situational causes that are responsible for our behaviour, because individual behaviour changes according to the circumstances of the situation in which people find themselves. It means 'you become what you need to become based on the situation you are in' espoused as 'the Lucifer Effect' and vulnerability to be tempted to 'the dark side' (Funder 2006; Funder & Colvin 1991). Studies by Barrett et al. (2013) have considered adoptive behaviour in the event of a crisis through a synthetic information and modelling environment which can allow policy makers to study various counter-factual experiments. The work considered a ground detonation caused by an improvised nuclear device in a large urban region. The importance of this work is the presentation of what they call the 'behaviour module' which shows that behaviour can be executed at various stages from rational (shelter seeking) to irrational (panic). When applied to computer failure situations, this same model would be useful in showing that smart and targeted interventions may influence situational behaviour and lead to improved outcomes. We therefore expand the person-situation debate into computer failure situations by exploring the phenomenon of exigencies in real-life situations that are aligned with shaping behaviour, and in doing so, explore possibilities of understanding of what it means to be an individual facing an ISec crisis. New insights will then serve as important considerations for understanding ISec behaviour in situations of crisis. We explain how we explored the phenomenon of exigencies in computer failure in the sections that follow.

4. Research Methodology

The research was qualitative, and the methodology applied for the study was phenomenological, with the underlying philosophical assumptions being constructive and interpretivist. We were guided by the need

to understand the phenomenon of exigencies in computer failure situations in its natural setting. These natural settings were to be considered as socially constructed. Following on the interpretivist paradigm, our conclusions are based on the interpretation of information obtained from participants, while being conscious and thoughtful of the individual meanings attached to their ISec behaviour (Crotty 1998; Sarantakos 2013). For qualitative research, the importance lies in the meanings, experiences and views of individuals (Pope & Mays 1995). We agree with Berger & Luckmann (1966) that it is through socialisation over time that a person gains knowledge, and that socialisation takes place in different communities under different circumstances, where a person shares, sustains and engages knowledge to construct 'multiple realities'.

This work is contrasted with other qualitative work such as action research, ethnography and grounded theory (Dowling 2007; Glaser & Strauss 1965; Moustakas 1994; Reiners 2012). In observing the different methods of qualitative research, the intention of this work was not to build a theory based on data gathered, such as expected with grounded theory research, but rather as a phenomenological study, the focus was primarily on people who experienced a phenomenon under study. Whereas phenomenology and Grounded Theory (Glaser & Strauss 1965) research may have some similarities, it is the philosophical and theoretical bases of the two methodologies and their influence on how research is undertaken that clearly differentiates one from the other. Each of the two approaches explores the experiences of people in a real-life context, are constructivist approaches by nature and have many interactions between the researcher and the co-researchers. However what makes this study important is that of performing an *epoche* or bracketing (Husserl 1983). The *epoche* lies at the heart of phenomenological studies and is explained in the next section.

4.1. Phenomenology research

Originating from the Greek word 'phaenesthai', the word 'phenomenon' means to show or to appear (Moustakas 1994). Considered the forefather of phenomenology, Edmund Husserl supported philosophy as an ultimate discipline, with an epistemological objective that linked to the question of 'How do we know it?' (Dowling 2007; Paley 1997; Ray 1994). Husserl (1983) believed that humans live in a natural

frame of mind, where ‘natural’ refers to authentic and naïve (van Manen 1990). Husserl referred to the ‘life-world’ (1983), a concept that went practically unknown during his lifespan until some of his unpublished manuscripts were studied (Spiegelberg 1971). The term ‘life-world’ is the events that we experience and live through before we contemplate and resort to analyses of the events (Dowling 2007). Husserl’s philosophy also included an additional concept of ‘phenomenological reduction’, which was fundamental to his epistemological strategy regarding descriptions of real-world experiences (Dowling 2007). Phenomenological reduction requires researchers to withhold their pre-judgements of the phenomenon and to ‘step outside the natural attitude’, which is attained by performing *epoche* or bracketing (Husserl 1983). There are uniform features that make a phenomenon what it is and the researcher must question each invariant feature and determine if the phenomenon will still be the same phenomenon if the feature was not there (Crotty 1998). As a qualitative method, phenomenology helps in achieving the objective of this study to determining through an *epoche*, how the exigencies of computer system failure situations would influence employee information security behaviour, through eliciting real-world verbatim accounts of research participants’ experiences.

4.2. Case Selection

The ideal organisation, which employed over eight thousand employees, was selected based on the availability of research participants as well as logistical considerations and importantly, that the researcher would be able to build relationships of trust with participants, as well as ethically conduct and report on the study (Marshall & Rossman 2011). Prior ethical clearance and consent was obtained before formal communication was initiated with, and personal visits to, the site. The benefits of the study were articulated to the participants as well as how the research would add value to the organisation from the insights generated. Anonymity and confidentiality were guaranteed via the signing of a legal agreement between the lead researcher and the participating organisation. The organisation granted us leave to interview and audio-record co-researchers selected for the study, as well as authorisation to publish the findings.

The South African organisation that agreed to participate in this study, is an entertainment services organisation that falls within the broadcasting and entertainment services industry. Operating under six

different brands, each brand functions as its own entity, yet contributes to the overall group. Each brand operates as an individual business unit. Singly, a brand contains its own functional departments within their business unit and is physically located at different sites.

Research participants were selected using preselected criteria that involved, firstly, identifying those participants that would likely provide unique and significant information that would meet study objectives. Secondly, the participants had to have spent sufficient time within the organisation to have acquired adequate knowledge and unique multiple experiences of computer hardware, software and network failure situations (Bordens & Abbott 2010; Mack et al. 2005).

4.3. Interviews and Researcher’ s Epoche

A letter of invitation to participate was emailed to participants who were recruited based on recommendations. An initial pre-interview contact session, via a formal appointment, was used to determine if the participants satisfied the study’s selection criteria of being an employee for a minimum of three years, using a computer on a daily basis, and keen to share their knowledge and experiences. Then semi-structured interviews were carried out. The preliminary interview instrument and some excerpts from the first two participants were interrogated to ensure both served the purpose of meeting the research objectives (Tanggaard 2009). After confirming that the interview instrument was successful in gathering the correct data, the rest of the participants were interviewed. In total, 12 participants were interviewed.

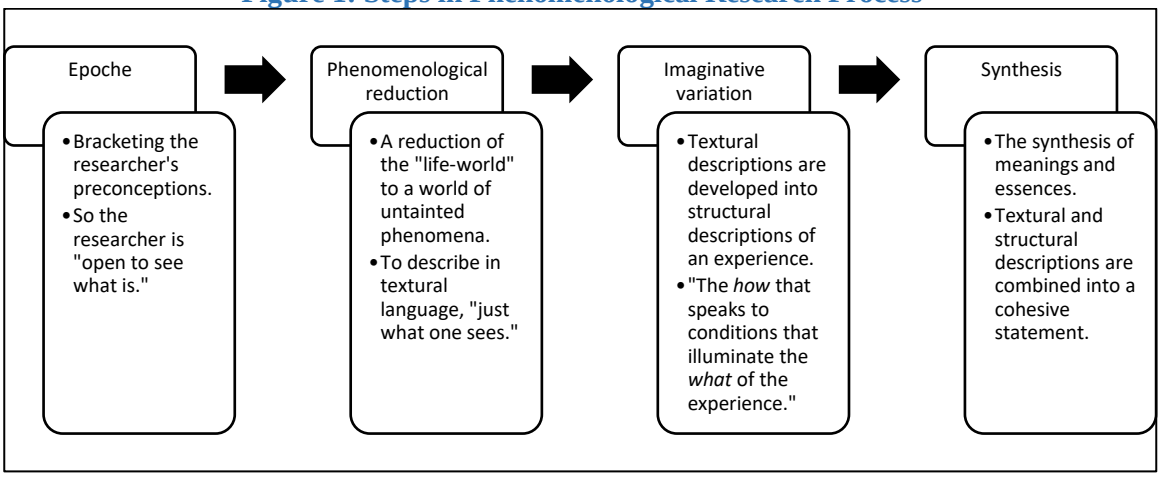
The main interview questions and prompts gathered information about employees’ experiences of computer system failure situations, how employees describe the exigencies of computer system failure situations, and how employees explain their behaviour in response to computer system failure situations. Each research participant was required to sign a release form and only after this did interviews commence. The interviews started with a social conversation (Moustakas 1994) to create an atmosphere that was relaxing and trusting. Demographic information was collected, followed by questions and prodding meant to elicit rich insights regarding each participant’s unique experience, regarding crisis and situations of computer failure. The research took cognisance of data saturation (Fusch & Ness 2015) and was guided

by the need to know how much data was needed and the limits that nothing new was being generated (Francis et al. 2010; Guest et al. 2006). All participants completed their interviews, with none opting to withdraw their data during the twenty-four-hour grace period that was given after their interview. Interviews were transcribed verbatim from the recorded audio files, and an email of appreciation was sent to each participant after the end of an interview session.

4.4. Steps in Phenomenological research process

The first step in Moustakas' process of phenomenological data analysis, brackets the researcher's preconceptions of the phenomenon under investigation. This is called *epoche* or bracketing. Bracketing one's preconceptions is an important aspect, because central to the phenomenological approach, is that researchers must persist in staying factual, and respect the manner in which the facts reveal themselves (Husserl 1983). *Epoche* involves the researcher stepping 'outside the natural attitude' to view the phenomenon in a fresh way, by not holding knowledge in judgement (Husserl 1983). Moustakas' phenomenology also includes the concept of 'phenomenological reduction', which is fundamental to Moustakas' epistemological strategy that requires a reduction of the '*life-world*' to a world of untainted phenomena (Dowling 2007). The end result of phenomenological reduction is to describe in textural language 'just what one sees (Moustakas 1994). Imaginative variation follows from phenomenological reduction, and the aim is to relate the important structures of the phenomenon, where textural and structural descriptions are developed from core themes. The main factors lead to an explanation of *what* was being experienced, and the conditions of what was experienced, by understanding *how* it was experienced (Moustakas 1994). The final step in the phenomenological analysis process is the synthesis of meanings and essences. This is when textural and structural descriptions are combined into a cohesive account of the essence of the experience of the phenomenon, in its totality that represents the whole group. These steps are described by Figure 1.

Figure 1: Steps in Phenomenological Research Process



4.5. Rigor

The research design of the present study followed a systematic and deliberate process to engage a research design that was complex and interrelated. Rigor was established through credibility, transferability, confirmability and dependability (Guba 1981). The researchers placed importance in identifying and documenting recurrent features such as patterns, themes, and values on the phenomenon under study. The main researcher also spend sufficient time with research participants and a 'submersion in the research setting' to identify reappearing patterns, to ensure credibility (Lincoln & Guba 1985). The researchers spent time to ensure the background information pertaining to the study and the phenomenon under investigation was comprehensive to enable the reader to achieve a transference (Firestone 1993; Lincoln & Guba 1985). The current study ensured confirmability by using thick descriptions of both site and phenomenon, which enables the reader to relate the study's findings to their own context. As much as possible, the researchers endeavoured to accurately detail the research processes to enable other researchers to replicate the work (Lincoln & Guba 1985; Shenton 2004).

4.6. Ethical Considerations

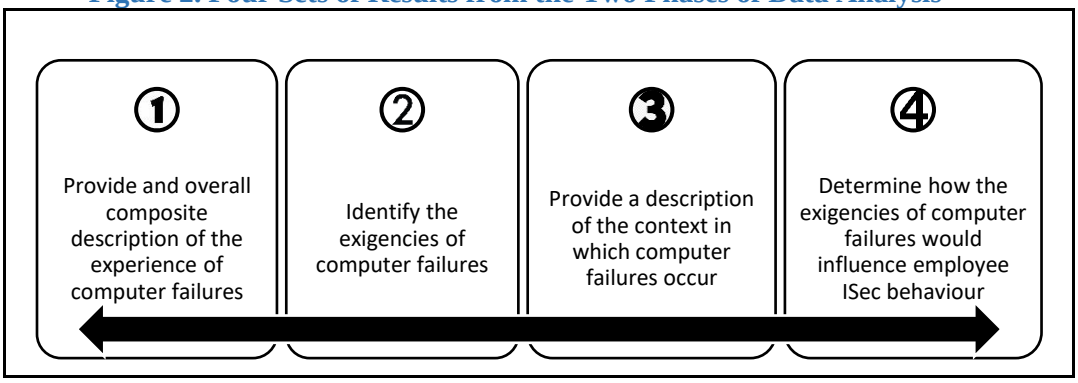
Ethical clearance was granted prior to commencement of study. We also made sure not to abuse supervisory authority, and to remain cognisant of conflicts of interests. From the outset, the researcher-co-researcher relationship in the present study was confidential, so as not to impair the relationship. Co-researchers chose pseudo names for themselves, which disguised their real names from everyone, except

me. We further guaranteed confidentiality by ensuring information was stored in a limited access, secure place. The limits of confidentiality in coding were discussed, and we confirmed that the confidentiality of shared results would also be maintained. Privacy was agreed on through informed consent, which established that no interview results could be linked to any specific co-researcher.

5. Data Analysis

Data was analysed to meet the objectives of study by applying Moustakas' four step phenomenological approach (Moustakas 1994). In this approach, the analysed data met the following criteria: provides a composite description of the experiences; identifies the exigencies of situations; provides a description of the context these situations occur and importantly; determines how the exigencies influence behaviour. These four phases are shown by Figure 2.

Figure 2. Four Sets of Results from the Two Phases of Data Analysis



After these four sets of results were completed, what followed was a summative assessment. The next section continuous to present the four sets of results, followed by a summative assessment of interview data.

5.1. Research Participants Profiles

Each co-researcher *selected their own pseudonym.* Co-researcher profiles, developed from the descriptions, indicate that co-researchers shared their knowledge about the ISPs, where to find it, whether they read it, together with their overall impression and experience when they had to deal with IT Support. This is shown by Table 1. Direct quotations from co-researchers enhance each description (See Appendix).

Table 1: Research Participants Profiles

Participant	Gender		**Duration in Organisation**	**Occupational involvement with Technology**	**Technology in Use**	
	Male	Female			**Macintosh**	**Windows**
Sakkie	X		4 years	IT-related role		X
Demi		X	16 years	Non-IT-related role	X	
The Big Guy	X		15 years	Non-IT-related role	X	
Charmaine		X	4 ½ years	Non-IT-related role	X	
CO123		X	20 years	Non-IT-related role		X
RMAC	X		16 years	Non-IT-related role		X
Goldberg	X		3 years	IT-related role		X
Starlord	X		8 years	IT-related role	X	
Mrs Philander		X	6 years	Non-IT-related role		X
Mary		X	9 years	Non-IT-related role		X
NodeCore	X		6 years	Non-IT-related role	X	
Grace		X	6 ½ years	Non-IT-related role	X	

5.2. Horizontalization

Every expression emanating from the above research participants pertinent to the phenomenon of computer system failure situations was considered, tested against a set of requirements and then such an expression became a *horizon of the experience*. One-hundred-and-forty-eight horizontalized expressions were extracted. The next section explains this process.

5.3. Invariant constituents, thematic labels, and core themes

The list of horizontalized expressions are refined by re-evaluating them again and removing expressions that are deemed irrelevant to the topic under investigation. This process refined the list to 123 invariant constituents of the experience, which was evaluated and thematically labelled. Thematic labels totalled 20, and application of thematic labels to invariant constituents is tabled. From the 20 thematic labels, five clustered thematic labels, with their corresponding invariant constituents that identified a core theme, are presented as follows: *computer failure diversity*, *emotionally stressful*, *computer failure management*, *problematic internal support*, and ad*ditional computer competencies*. Table 2 is a summary of the 20 thematic labels, their meaning and related core themes.

Table 2. Thematic Labels and Core Themes

Core Themes	Meaning	Thematic Labels
Computer failure diversity	Co-researchers experienced computer system failure situations as a diverse set of hardware, software, and network failure situations.	1. Internet network access problems *(Table 3)* 2. Intranet network access problems 3. Network password resetting problems 4. Problems with printing 5. Problems obtaining license keys for specialised software 6. Procurement of new hardware
Emotion	During computer system failure situations, co-researchers felt very frustrated and negative, because they have a task that needs to be completed at all costs. The lack of consequences only adds to the stress of the situation because they are uncertain as to when they are transgressing policy.	7. Frustrated *(Table 3)* 8. Negative 9. Urgent 10. Having duty 11. Lacking consequences
Computer failure management	Co-researchers must manage computer system failure situations, over and above their normal daily duties, in an environment where IT Support is their last resort.	12. Over and above daily duties *(Table 3)* 13. IT Support is the last resort
Problematic internal support	Co-researchers must interact multiple times with substandard internal support to obtain help with recurring computer system failure situations	14. Multiple follow-ups *(Table 3)* 15. No feedback 16. Took very long 17. Sometimes unresolved 18. Reassigned multiple times
Additional computer competencies	Co-researchers must find new or use existing, justifiable workarounds, or sometimes even revert to asking a colleague for help.	19. Self-produced resolutions *(Table 3)* 20. Not for personal gain

The 20 thematic labels are each uniquely supported by concise invariant constituents directly from participants own words that are presented as evidence. As an example, we present one thematic label from each core theme and illustrate how rigor was applied towards identifying concise invariant constituents. This is shown by Table 3.

Table 3. Extract and Evidence for Computer failure diversity

Meaning	Thematic label	Evidence from concise invariant constituents
Computer failure diversity	Internet network access problems (Table 2)	*'It's a problem where our outgoing Internet connection gets saturated. . . it gets to a point where we can't do our work'.*
Emotion	Frustrated (Table 2)	*'Another frustration [when] dealing with someone [inexperienced]. . .'*
Computer failure management	Over and above daily duties (Table 2)	*'. . . the first thing I do is to inform my manager. I can't do my work, if you want me to do my work, you need to provide me with better equipment. The case as it is my manager can't do anything*

		about it as well. So, it will need a further escalation process'.
Problematic internal support	Multiple follow-ups (Table 2)	*'You keep on following up and following up and eventually you get an answer saying, we are experiencing problems, we are working on it, we don't know when it will be fixed. That is where it will basically end'.*
Additional computer competencies	Self-produced resolutions (Table 2)	*'. . . other people in our team, having the same problem. . . I use my own private phone, so that they can connect to my phone and just do whatever they need to do, because the 3G stick that I have, is the company's 3G stick that they use for Macs. For some reason you can't use that thing on the Mac. So, I let them connect to my mobile device, to help them do whatever it is they need to do'.*

In the context of this study, when co-researchers experience a diverse set of computer system failure situations, they are experiencing various kinds of computer system failure situations. The challenge with managing computer system failure situations, is that research participants need to get the situations resolved in difficult circumstances, where it is a problem to find proper internal support from their IT service desk. Co-researchers must interact multiple times with internal support to obtain help with recurring computer system failure situations**.** This require of them to find their own solutions to problems, which in turn necessitate the acquisition of additional skills, usually unrelated to their job description. To present a detailed analysis regarding how we arrived at the composite description of the phenomenon, the following sections elaborate further on *textural descriptions*, *structural descriptions*, and *textural-structural descriptions* of the participants situational experiences and exigencies. The experiences of four participants are detailed in the section that follows.

6. Textual Descriptions

Each textural description provides interesting and diverse perspectives of situational exigencies by explaining each research participant's experience. Descriptions are rooted in invariant constituents, core themes and verbatim examples from transcribed interviews. From the 12 interviews with research participants, four dialogues have been selected for analysis that are an all-inclusive representation of the rest of the research participants' experiences. We explain each of these four in the section.

6.1. Sakkie' s Experience

Sakkie recalled his first experience with the organisation's IT Support, when he was a new employee and

needed network login details. After completing all requirements and submitting it to IT Support, nothing happened.

> *'The first time I phoned IT Support, they said I need a new user ID. I filled in the new user form. . . got my manager to sign the forms [to] approve the request. I sent it in and never received any response back'.*

This first experience was to set a trend for any further fascinating interactions between Sakkie and IT support when logging incidents. The culmination of the past four years of, Sakkie's experiences with IT Support would include but not limited to: not receiving feedback after an incident was logged; follow up about logged incidents multiple times with little assistance; incidences that were reassigned multiple times, incidences that took very long to be resolved; and sometimes facing unresolved incidences.

Sakkie found that with more complicated computer system failure requests, he was unable to rely on IT Support to help him:

> *'If I phone IT now and say I want a network printer, they either assist me over the phone or they say someone will come to your desk in the next few hours. . . but if you go into more detail IT stuff, like internal blocking of IP addresses. . . you can't really rely on them. But your normal day-to-day, desktop support from IT, is great. The more advanced IT stuff, I'd say is difficult to rely on'.*

Overall, Sakkie found these experiences '*very frustrating*'. This however was not the end of these frustrations:

> *'Another frustration [is when] dealing with someone [inexperienced]. . .'*

An important source of frustration was when the 'inexperienced' IT support would take a long time to resolve problems with some of the problems remaining unresolved.

> *'This other person that has been sitting here since January, still do not have any access to our network, he is using someone else's credentials to log in. So, someone from his 3rd party company, who has login details that actually isn't here anymore. That used to be here Monday to Friday, but he is not anymore. He is using this other person's credentials to log in'.*

One of the more critical problem that kept recurring and remained unresolved was connectivity to the Internet. Obtaining and keeping an Internet connection was a challenge that kept IT support from doing their work.

> *'Anything that's on an international server or outgoing connection, it gets to a point where we can't do our work. It's a problem where our outgoing Internet connection gets saturated'.*

Sakkie continued to explain that '*in the mornings it's OK*', somewhere between 6am and 8am in the morning and '*again from 5pm*', it starts to ease up again. He explained that it would take most of the day to download a large file.

> *'If I had to download a file, let's say a Gig, it will take most of the day, there are just way too many people on the Internet in this building'.*

Another regular problem was an unavailable internal network, and Sakkie had to revert to using his own Internet connection using a 3G stick.

> *'Today, for instance, I'm not able to do my work from the network. I have to use a 3G stick to do my work. I can't use the internal network. So that's just the normal network in the building. . . is such a problem that I can't do my work'.*

Sakkie mentioned that he would not be able to do his work, but he would be able to watch YouTube videos.

> *'What they have done is, I think about two months ago, they sent an email saying that they are going to lower the priority of YouTube on the network. I can go on YouTube now, I can play you a video, but I can't do my work on the intranet'.*

Sakkie always informed his manager when this problem occurred and would improvise by working from home.

> *'It's easier for me to stay at home and work from my home network than be at the office and try and work on this network'.*

As a result of these culminating long-term frustrations, Sakkie's character and behaviours would gradually start changing based on these situations and as days would go by, he would slowly start finding himself unintentionally violating security policies. He would start allowing other employees to use his own private Internet by Hot Spotting them from his phone.

> *'it even went to the extent that other people in our team, having the same problem, that I use my own private phone, so that they can connect to my phone and just do whatever they need to do. So, I let them connect to my mobile device, to help them do whatever it is they need to do'.*

As his experiences unfolded, it was becoming clear that Sakkie was a changed person from who he was initially in his first days of working. What was observed is that as the frustrations and exigencies in situations pilled-up, he would now blur the line between following ISPs. This was evidenced from his

recollection regarding downloading unlicensed software. When he was allocated a new laptop, he requested the installation of the required specialised software as well. When the laptop was delivered to him, he found only half of the requests were fulfilled.

> *'Over time I had a few software installations with licenses. When I received a new laptop, I sent an email to IT, saying that when they setup my new laptop, that I need specialised software installed on it and that there were license keys bought for me a few years ago. When the new laptop was returned to me, with only half of the required software, it was such a mission to get it all back on'.*

With missing software, he ended up doing whatever he could to make his job easier and better.

> *'I downloaded software myself. I first tried IT, then they said I must ask this person. I asked this person and then he said no, he does not have any licenses for me. Then I figured if their support desk doesn't know about it, and the person that is supposed to have it, doesn't know about it, who do I contact now? And the people at that time, when I got all the license keys, aren't even working at the company anymore. I am sure if I go to my manager now and say I need this right now, the process to get it, it needs to be approved here, then approved there. There are so many people that need to give approval that it's going to take very long to actually get it. It's then easier for me to just go and do it myself. Obtain software from a 3rd party website'.*

6.2. Textual Themes from Sakkie's Experience

Six textural themes emerged from Sakkie's experiences of computer system failure situations that accounted for his emergent behaviour: 1) the problem of finding proper internal support when situations occurred; 2) the emotional stress, especially frustration, that he went through during such situations; 3) the number of recurring, unresolved situations that he had to deal with over and above his daily job; 4) his ability to find alternative solutions himself; 5) lack of enforcement of Information security policy; and 6) just getting the job done.

6.3. Demi's Experience

Demi joined her organisation 16 years back. Her initial perception regarding IT Support was not impressive:

> *'It is as if they practically do not exist. . . in general, there wasn't much of an IT Support when I first started here'* and that her experience with them *'wasn't always great'*.

This perception would gradually change over the years and Demi's impression of them improved.

> *'I think with the move toward Mac, the IT department kind of spruced-up their knowledge of Mac and what works on the network and what doesn't. . . They have some specialists now'.*

Demi explained that when computer system failure situations occurred, she would first attempt to solve a problem herself, using every workaround possible. It was 'when all else failed' that she would be forced to contact IT Support.

> *'I usually tend to start with myself first. . . I've found workarounds. . . I try every possible solution myself. I will go to IT as a last resort, because once you've logged a request, it doesn't mean that they come running to solve your problem. They normally take a couple of hours or days to come'.*

Contributing further to the stress experienced during computer failure crisis, was the timing of the occurrences particularly when urgent tasks needed to be completed.

> *'I normally find that I have problems when I need to get stuff done urgently. I'm in the wrong state of mind when it's happening. If it happens when I was having just a normal day, then usually it is fine, but this is when somebody needs a presentation delivered urgently or something needs to be printed in colour urgently'.*

A prevailing stress factor for Demi was usually from the organisation's internal network. In one incident that she recollected, she needed to access big files on a regular basis, but as a Mac user, she found her access was blocked.

> *'The internal network gives us a lot of issues. Normally we just work on the company Wi-Fi now. The network is extremely slow and it is very restrictive in terms of what you can access. . . I need to access big files. But I can't do that with my Mac on the network, it blocks me'.*

Also, as a manager, Demi had different departments that reported to her and she thus needed to perform network related tasks such as managing personnel leave applications and performance reviews. Without a stable network connection, she felt frustrated when she was unable to perform these tasks.

> *'Even as management, to approve leave from my side, manage performance documents and all of that stuff, you need to be on the network. . . I'm swopping between a network cable and switching on Wi-Fi, and switching off Wi-Fi. . . 'It's very frustrating. It adds to the stress of the current situation, of having to deliver'.*

When Demi was not busy plugging in and unplugging cables, she tried to be proactive and on account of being too over reliant on IT support, would troubleshoot tasks such as password reset on her own.

> *'I've got to be proactive, with something which is usually quite simple to do on a Dell [and not Mac] . . . On a Windows-based computer, a pop-up appears that says your password has expired and you should change it. . . it just changes everywhere. . . but unfortunately. . . it doesn't work like that on a Mac. . . On my laptop, if my password expires, which it does often, I think it is every 5 or 6 weeks. . . It causes a huge panic. . . everything goes out of sync, and it won't allow me to change certain passwords'.*

Eventually Demi figured out that by setting reminders on her calendar to reset her password before it expired, this would resolve going out of sync on expiry.

> *'I've saved something in my calendar, saying something like, don't forget to change your password. . . because if I am not proactive enough, I missed it and it has expired, then it is a huge problem. . . 3 days of headaches'.*

Demi mentioned that she was not the only person using workarounds and that other people also found their own workarounds when they experienced computer failure. She did, however, endeavour to stay within the ISP guidelines, and would not transgress policy on purpose.

> *'There are people that have found ways around it. . .. I do try and stay within the parameters of the organisation'.*

In one occurrence, Demi downloaded a free imaging tool known as 'GIMP' to replace Photoshop that she was unable to retrieve from her machine.

> *'I've always had Photoshop and development tools on my Dell machine. Moving into [name withheld] and getting a Mac, it removed me completely. So, I started fresh on a different operating system and it wasn't working properly and the network at that stage. . . I would have been able to resolve any of the problems on my Dell, within the parameters of what we were given, but with Mac, I need Photoshop. . . I can't get Photoshop, because they have limited licenses. So, what I did, I went and download GIMP, which is a free imaging tool. I've downloaded quite a couple of other tools that work between my Mac and my iPhone'.*

Demi found that there were many grey areas regarding standard operational procedure for third party software installation. She did not consider that the software downloads were outside the security parameters of acceptable software considering these were '*free tools*' and did not think that the organisation would audit '*that kind of stuff*'. Her perception was that the organisation was inconsistent in policy enforcement, since, '*some people got away with transgressing information security policies'*.

> *'I find them inconsistent. In general, I think. . . when you join you have to sign the security and what's going to happen. What you can browse and what you can't, but the problem with that is, there are people that have found ways around it, and I just find that they are not punished for what they've done or found. In general, for most people it's fine, but for the people that found ways around it, they've been able to get away with it. . . [there is] a lot of grey areas still'.*

6.4. Textual Themes from Demi's Experience

Five textural themes emerged from Demi's experience of computer system failure situations that accounted for her behaviour during said situations: 1) the difficulty for her using IT Support procedures that did not

work properly; 2) the emotional stress, especially frustration, that she went through; 3) having alternative options in the form of workarounds to solve computer system failure situations; 4) the number of situations that she had to deal with; 4) inconsistent enforcement of Information security policy and acceptable grey areas to work in; and 5) having to deliver.

6.5. The Big Guy's Experience

The Big Guy has been with the organisation for 15 years. As far as his interaction with the organisation's IT support goes, '*it has come a long way*'. Overall, his impression was that they have '*improved their service levels quite significantly especially in the last year'*. Whereas the organisation traditionally had a relatively good IT Support function, this was not the case for those who required Macintosh (Mac) support. The Big Guy thought that

> *'Support for PC is better than Mac, but Mac support. . . it's come a long way. I don't think they (IT) support Mac as well as they support PC'.*

His experience with plugging his Mac into the different LAN, Wi-Fi, and VPN platforms, was as follows:

> *'The proxy just kind of goes crazy. . . I don't plug in the LAN. . . I haven't plugged into the LAN for quite some time. . . my last resort is plugging into the LAN'. About the Wi-Fi, he lamented 'you always have to ask, is the Wi-Fi down'.*

The Big Guy vividly remembered an experience once, where he was unable to log into the organisational portal using the Wi-Fi for an appraisal that was due.

> *'I can't log into that portal via the Wi-Fi, even though the Wi-Fi is domain and active directory specific. . . so I log into the VPN, to get access. . . unfortunately [after logging in] the browsing is extremely slow, where every 15 seconds the connection drops, but it doesn't log you out. You can't do anything on the browser. . . you click on something and then it chucks away for 15 seconds, and then it catches up'.*

The Wi-Fi crisis was exacerbated further when The Big Guy found his access credentials were not recognised.

> *'A recurring incident is when your access credentials to the Wi-Fi are not recognised. Generally it is a case of either your account is locked or your password has expired. . .the service desk. . . says that if your password has expired, go to this website. . . which you can't go to, because you can't log in to the Wi-Fi, so it doesn't really help'.*

The Big Guy resorted to using a hotspot to access the website. '*You actually hotspot, which sometimes I do*'.

The Big Guy described the emotional experience of computer failure as a crisis filled with '*a range of emotions, and none of them are good'.* Describing himself as feeling '*irritated*', '*helpless*' and sometimes even having emotions that bordered on '*fear'*. The Big Guy's recollection of these emotions is expressed by the following:

> *'You've got to do something functional, something that your job requires you to do, and now suddenly you can't do it. You are irritated, and once you've gotten over that, you feel quite helpless. . . you are just helpless in the situation. It really is quite irritating. The major is irritation, but sometimes also fear, because now you could get into trouble, miss out on your deadline'.*

In a similar occurrence, The Big Guy wanted to book a boardroom for a meeting that ended up in an emotional roller-coaster that propelled him to '*make a plan. . . you've got to make a plan*'.

> *'It always happens when you are under pressure or have a deadline. When you've got to book a meeting room for example. It normally happens then, not when you've got a few moments. It happens when you really need it because you've got the get onto the network. What are you going to say, no sorry I couldn't get onto the domain that is not going to fly? Those are just not acceptable excuses'.*

During moments of crisis, the last thing on one's mind, as The Big Guy recollects is following ISPs.

> *'I don't even think about it [information security policies] at that point. I just have to get the job done. Whatever I need to do, I've got to make it happen. . .. [these policies] a little bit confusing. . . It's not explicit to me, when and under which conditions, I violate the IT policy. . . I think that if there is something I need to do for work purposes, then I wouldn't even think twice about it, and if the company gave me a written warning because I did something that violates some policy, but it was a proper reason for work, I would probably fight that written warning'.*

6.6. Textual Themes from The Big Guy's Experience

Six textural themes emerged from The Big Guy's experiences of computer system failure situations that accounted for his behaviour during said situations: 1) the problem of finding proper support when situations occurred; 2) the number of recurring situations that had to be managed; 3) the emotional stress, feeling irritated, helpless and sometimes even fear; 4) having his own alternative workarounds to solve computer system failure situations; 5) being unable to perform what was expected of him; and 6) confusing Information security policies, especially as to when he was actually transgressing policy.

6.7. Charmaine’ s Experience

Charmaine had only been with the organisation for about 4 ½ years and found IT Support helpful, especially in respect to her experience of logging calls regarding incidents. However, this experience was different when someone had to literally come to her desk to resolve issues. According to her, the wait would be quite long.

> *‘So, our helpdesk is twenty-four hours and they are really helpful and all of that. We do sometimes wait for quite a while for someone to come help you. . . you are at the mercy of when the person has time to come to you’.*

During crisis situations, Charmaine would often request assistance from her manager to help escalate incidents, particularly when she was unable to regularly follow up on an unresolved issue and recalls frustration.

> *‘I’d probably go to my manager. . . get my manager involved. . . because you forget about it and then you need to do something and then you remember about it again. . . this process [is] very frustrating’.*

For Charmaine, crisis situations that have ended up causing the most frustration was for her having to change her password as well as being unable to print.

> *‘With the password, think that for me truly that one is the one that kills me because it affects me one hundred percent. . . it is a great source of irritation [when] it takes so much of my time to do something simple’.*

What was in her experience irritating and has occasionally made her almost ‘*lose her mind*’ is when she would receive the password change email notification.

> *‘What happens is you get a notification that your password is going to expire so you change it yourself. . . after a simple restart of the computer, you would think that you’d be done, your password would be changed and you would be good. . . [but]. . . it doesn’t. . . a message would say that it has changed. . . [and you] shut down and come back on, then the computer] does not let me in. . . it has happened a number of times’.*

In one experience this crisis was so prolonged, that she ‘*couldn’t do anything for three days*’. In similar experience, that elicited almost a similar emotion was a day she recollects that had been unable to print because she was a Mac user. She resorted to asking a colleague for assistance.

> *‘I couldn’t print [because] IT couldn’t figure out putting me on a printer. . . my boss and I yesterday had the same conversation he can’t print either. . . I’ve now resorted to asking [person’s name withheld] actually printing for me’.*

According to Charmaine the crisis was avoidable since it wasn't so much a Mac problem as it was a '*lack of skills within a department*' problem.

> *'Sometimes it will work for like a day and then it stops working, the one guy couldn't get it right at all. Macs are a problem. . . that's what they say. I think it's an excuse. I think it's a lack of skills to be honest with you. . . if I lacked a skill like that within my job, I wouldn't have a job'.*

In another crisis situation, recollected by Charmaine, was when she had struggled to obtain the Photoshop software. Initially, obtaining approval and placing the order would not be a problem. The problem and resultant crisis was when months passed by and she was yet to receive the software.

> *'I need Photoshop because we work with images and that kind of thing. . .. the quote was approved by my manager and I still don't have Photoshop. . . we have waited now three or four months'.*

Following up with IT Support did not produce any results, causing her much frustration.

> *'The Photoshop thing it obviously frustrates me. It's just something that irritates me that I need to sort out'.*

Charmaine would eventually find a 'skilled' person who '*knew what he was doing'*.

> *'I found this guy who then. . . he fixed it and now I'm fine, now I can change my password by myself no issues. . .. I went through hell before I found him. . . it took about four incidents. . . and . . . two or three people later. . . but it was a very frustrating process'.*

She now requests him to personally oversee her issues as they arise and whenever she has a problem. She has found herself in a position where she now has a contact at IT Support that helps.

6.8. Textual Themes from Charmaine's Experience

Five textural themes emerged from Charmaine's experience of computer system failure situations that accounted for her behaviour during said situations: 1) the problem of delayed response between logging an incident and waiting for IT Support to fix it; 2) IT Support procedures for users that did not work properly; 3) the emotional stress, feeling frustrated and irritated; 4) the number of recurring situations that had to be coped with; and 5) having found that one IT Support person that she contacted exclusively, bypassing IT procedure, and opting to use workarounds if she had them.

7. Composite Textual Description from all Four Composite Textual Descriptions from all Four Description from all Four Research Participants

We collocate experiences from the four research participants and apply the composite textual description

commonly used in phenomenological studies to unify these experiences are summarised by Table 8.

Table 8. Summary of Experiences

Research Participant	Summary of Textual Themes
Sakkie's Experience	• lack of proper internal support • emotional stress • recurring, unresolved situations • ability to find alternative solutions himself • lack of enforcement of ISec policy • getting the job done
Demi's Experience	• difficulty using IT Support procedures • emotional stress • followed her own alternative and used workarounds • numerous situations to deal with • grey areas and inconsistency in ISec policy enforcement
The Big Guy's Experience	• the problem of finding proper support • recurring situations • emotional stress, irritated, helpless and fear • followed his own alternative and used workarounds • unable to perform tasks • confusing ISPs
Charmaine's Experience	• delayed response for IT Support • IT Support procedures not working properly • the emotional stress, feeling frustrated and irritated • recurring situations • bypassing IT procedures by embracing workarounds

Most research participants agree that these moments of crisis were emotionally stressful with the level of stress escalating significantly when there was an added element of urgency to the situation. Most were frustrated as well as irritated with some feeling helpless at times. It the case of Sakkie, these exigencies in situations of crisis would culminate to observable behavioural changes from the person he once was. Stress during these situations was observed to manifest uniquely for each of the research participants. For some, the frustration was time taken to resolve the crisis while for others was in the fact that after the waiting, the person meant to assist could not be able to deliver. Emotional expressions ranged from feeling irritated, helpless as well as feeling fearful.

Research participants found moments of crisis caused by hardware, software or network failure challenging to manage and problematic to resolve. This made them have a difficult time performing their tasks. Hardware, software, or network failure ranged from not getting an outgoing connection, to having

a breakdown in an international server, to the internal Wi-Fi network being slow or restrictive as well as missing important software (such as Photoshop). A lot of energy and time was spent on workarounds and '*getting the job done*', motivated by wanting to deliver what was expected of them. Exigencies in these situations required behaviour change to manage these challenges over and above the normal call of duty. The unintended behaviour change caused by meeting these demands was for ISPs to inadvertently be overlooked and to therefore turn 'good people into bad'.

8. Structural Descriptions

Structural descriptions are rooted in phenomenological studies and advocate that the researcher uses imaginative variations that would represents the subtleties in textural qualities. Emphasis is placed on the *feelings and thoughts* connected to these situations. We present a discourse regarding structural descriptions for the four selected research participants in the section that follows.

8.1. Feelings and Thoughts from the Research Participants

Sakkie's feelings and thoughts in times of situations of crisis resulting from computer failure are expressed in emotions such as struggle. '*I'm struggling every day'.* The feeling of frustration was equally echoed particularly where simple tasks became '*such a mission*' and the burden of duty was great. For Sakkie, work meant duty, and the inability to manage and resolve crisis became a challenge that kept him from doing his work. '*Today for instance, I'm not able to do my work from the network. I can't use the internal network. . . it is such a problem that I can't do my work*. His sense of duty was articulated well here.

Demi's feelings and thoughts also expressed frustration and she described herself as being '*in the wrong state of mind when it's happening*'. Demi described her level of stress, increasing when failure occurred in times when urgent tasks needed to be completed. At times, these situations left her at the mercy of IT support and pointed out that IT Support '*needs a little bit of work from their side'.* Demi felt an ingrained sense of duty when performing tasks and delivering results. As a manager, she had different departments that reported to her. Duty she noted, is '*having to deliver*', but she struggled to do this in the face of constant network failures. Demi found that she spent a lot of time performing tasks that were both

needless, yet important. Such as constantly having to plug in and unplug from the network, which she should not have to be doing, but was required to do to perform tasks that needed a network connection or even printing. '*I'm swopping between a network cable and switching on Wi-Fi and switching off Wi-Fi. . . unplugging and plugging in all the time'.* Demi's sense of responsibility compelled her to be practical.

The Big Guy expressed an array of feelings and thoughts during situations of crisis and described the emotional experience as '*a range of emotions, and none of them [were] good*'. He felt irritated as well as helpless the moment these occurred and especially during critical moments. '*It really is quite irritating. . . You are irritated, and once you've gotten over that, you feel quite helpless*'. An interesting emotion that The Big Guy expressed was that of fear. The possibility of missing deadlines and '*getting into trouble*' was observed as the primary basis for such emotion. The Big Guy's emotions were intensified when deadlines were looming. His steadfastness as well as self-efficacy in managing this emotion is articulated by his reasoning: '*You've got to make a plan. . . whatever I need to do, I've got to make it happen. . . I don't even think about it at that point. I just have to get the job done'.*

Charmaine expressed deep frustration in moments of crisis resulting from computer failure. '*It is frustrating having to wait several days and when the person shows up, he/she is unable to resolve the problem. . . the frustration. . . you don't get the help you need, that's terrible*'. The emotions often elicited were profound to the point of breaking. '*. . . for me truly that one is the one that kills me because it affects me one hundred percent. . .'* She explained how a lifeline was thrown on one of those situations when she identified a specific IT support personal who would end up helping her in these circumstances.

8.2. Textural-Structural Synthesis

Computer system failure situations are experienced as disrupting the natural ebb and flow of one's usual workday. It disrupts by interrupting the natural rhythm of the incoming flow and outgoing ebb of activities, and it disrupts by causing emotional upset by creating moments of crisis. These moments of crisis interrupt the steadiness of normal daily activities, of performing daily tasks and delivering results. These situations call upon a sense of duty and require employees to carry out their duties over and above what is normally expected of them. Often these situations elicit emotions such as anger, stress, irritation frustration,

helplessness and sometimes fear.

Observing the emotions represented by research participants, there was a consensus that although these crisis situations were unpleasant, these exigencies were not legitimate excuses for not completing work. Most participants would be eager to seek remedial outcomes as soon as possible. These findings are in line with studies on crises related to IT (Huddleston & Pullum 2002). The studies found that in instances when an employee would find themselves without the necessary computing technology to perform certain tasks, they would find ways to continue working without. The next section discusses the exigencies of computer system failure situations.

9. Exigencies of Computer System Failure Situations

As part of computer system failure situations, there are certain things that employees must manage and boundaries within which they must work when computer system failure situations occur in their workplace environment. In determining the exigencies of said situations, we could gain an improved understanding of what inspires unique research participants' behaviour during these types of situations. It is very likely that individuals will act a certain way in a certain situation because there is something about the situation that prompts that behaviour (Furr & Funder 2018). For the purpose of reporting the findings from research participants' interviews about the exigencies of computer system failure situations, and explaining how employees describe the exigencies of computer system failure situations, we present five exigencies derived from thematic labels and core themes identified in the study. Of these five exigencies, one was identified as being of great significance and kept reoccurring as a point of discussion by each of the research participants, and this was emotional stress. The feeling of emotional stress, profoundly elicited other emotions such as tension and heightened frustration. We present and discuss each of the five exigencies are as follows:

9.1. Exigency 1: Diversity in computer failure situations requiring diverse management

An important proposition observed based on interviews from research participants is that in any typical organisation, employees will inevitably face situations of computer failure, and this must be managed in

diverse ways. Research participants mentioned having encountered different hardware, software and network failure situations which had to be managed. Literature supports the occurrence of multiple disruptive situations in the workplace and indicates that these situations are often found to be multifaceted. The possibility to differentiate situations from each other allows us to distinguish between similar situations. This could be accomplished by considering them as a set of comparable situations, with each comparable situation having its own goal and related tasks to accomplish that goal, thus characterised by its own features (Deutsch et al. 1994; Huddleston & Pullum 2002).

9.2. Exigency 2: The Challenge of managing computer failure

Research participants mentioned that it was challenging to manage crisis resulting from computer failure when crisis occurred suddenly. A crisis is a situation which happens suddenly, during the normal day-to-day routine, and which is in need of some action (Huddleston & Pullum 2002). Usually, crisis situations related to IT during technological failure will most probably cause disruptions (Coombs 1999; Huddleston & Pullum 2002; Lerbinger 1997). In the research participants perspectives', the crisis was exacerbated when failure interrupted normal duties and that IT support was found wanting. There was consensus by most research participants that internal IT Support would be their last resort in attempts to solve computer system failure situations. Most would rather attempt to resolve the problem themselves.

9.3. Exigency 3: Internal IT support's inadequacy

Most research participants professed the inadequacy of IT Support when requested to assist during moments of crisis caused by computer failure. The inadequacy was compounded by the difficulty research participants faced when logging in incidents, requiring multiple channels such as telephonic, email, web-based and face-to-face to be used. Lack of feedback and of having logged incidents that went unresolved proved daunting.

9.4. Exigency 4: Additional skilled competencies needed

A profound experience observed by research participants was that their typical IT support would need additional competencies, over and above their ordinary competencies. Since IT support was wanting,

research participants would find innovative or improvisational workarounds to resolve, albeit sometimes only temporarily, computer system failures. That employees would result to being improvisational to manage ISec incidents (Njenga & Brown 2012). Workarounds were perceived as not for personal gain but rather a sense of duty to the organisation. Studies show that risky and unclear situations found in the workplace require unexpected skills to resolve, compared to normal situations that are distinguished as monotonous, clear and effortlessly accomplished (Deutsch et al. 1994).

9.5. Exigency 5: Computer failure is an emotional construct

In important exigency observed is that emotions elicited during a crisis that may cloud rational approach to crisis. The construct of emotions during crisis has been documented by researchers in social sciences (Cohn et al. 2000). Codes and negative phrases used to describe emotions were documented and included; '*frustration*', '*irritation*', '*helpless*', '*upset*', '*stupid*', '*angry*', '*embarrassed*', '*a bit of a misery*', '*I felt like this big*', and '*fear*'. Social science studies have also used emotional constructs to describe how the individual perceives stressful situations (Rauthmann et al. 2015).

10. Discussion

Social Psychology's raison d'être is the notion that situations and their characteristics play a fundamental role in human behaviour (Baumeister & Tice 1985; Edwards & Templeton 2005; Meyer 2015). Situational characteristics can have a noteworthy influence on behaviour, cognitions, and emotions (Ross & Ward 1995). From the results, it shows that all five exigencies have an important effect on research participants as these were openly expressed during their interviews numerous times. Two of the exigencies are more significant than the other three. The most important exigency in our interpretations was the emotional stress experienced when crisis happened. The second most important exigency is when research participant had to manage flawed procedures and recurring problem on their own due to the internal IT support's inadequacy forcing them to be improvisational in their workarounds. The situational leg of Interactionism accepts that individual behaviour is influenced by the characteristics of a situation in which the behaviour takes place. It is very likely that individuals will act a certain way in a certain situation because there is

something about the situation that prompts that behaviour (Furr & Funder 2018). Each exigency was seen to affects research participants behaviour. Unique behaviour was noted to be elicited from the emotional stress of frustration (exigency 5); from flawed IT Support procedures and recurring problems (exigency 1); from IT Support taking too long to attend to crisis (exigency 3); from using workarounds to solve problems (exigency 4); and from being improvisational and offering own resolution to problems (exigency 2). All exigencies have an important effect on research participants behaviour, and within each exigency, there is an element or elements that are more significant in shaping ISec behaviour. We observed interesting ISec policy and how these would be violated in situations of crisis such as (1) intentional violation, (2) non-malicious violation, (3) volitional, and (4) non-compliant violation.

During moments of crisis, researcher participants would elucidate ISec behaviour that was non-malicious and but equally non-compliant to ISPs. Some would intentionally and knowingly engage in undesirable security behaviour by using workarounds. Some chose to break the rules, and rationalise the behaviour '*getting the job done, whatever it takes*', however behaviour was not documented as having malicious intent. For research participants, the best explanation for exhibiting intentional non-malicious behaviour during computer failure, appear to be the exigencies of the situation in which the behaviour takes place. As concluded by Situationists, an equitable explanation of behaviour is that it is caused by the situation (Candace 2009; Darley & Batson 1973).

10.1.Implication to Theory

One implication for theory is that there is an identified need to further investigate ISec behaviour of employees in different situations since employees have been observed as weak links to the security of information systems. For the scholarly community, the findings from this study extends knowledge in the existing body of behavioural ISec research regarding behaviour, by reinforcing the importance of the situation. Insight is provided into the exigencies resulting from crisis in computer failure situations and the context by which exigencies occur. This was previously undocumented in literature and this work now supports ISec studies that may place great significance on the situation and human behaviour. By providing rich insight into the exigencies of computer failure, the context exigencies occur, this work study extends

knowledge about of real-world experiences that expands our theoretical knowledge of this phenomenon.

10.2.Implications for Practice

For practice, several implications are highlighted. Emotional stress employees experience during computer system failure is noted to have the greatest influence on ISec behaviour. These situations are stressful and will elicit emotions. Practitioners should therefore perceive and deal with computer failure not as a physical occurrence and therefore a physical construct to be dealt with using physical interventions, but rather an emotional constructs where emotions such as frustration, irritation,, helplessness and fearful must be dealt with . Based on our findings, organisations are encouraged to facilitate optimal employee wellbeing in the workplace as fundamental intervention during computer failure. Employees should be endowed with the resources to manage their emotional wellness more effectively as well as have a workplace that is supportive when situations of crisis occur.

10.3.Study Limitations and Directions for Future Research

The study was qualitative, and a phenomenological approach designed to elicit research participants' real-world experience regarding computer failure situations. Phenomenological studies are subjective and will inherently encompass subjectivity and bias on two fronts: From the researcher as well as participant's viewpoints. Although this is not necessarily a weakness, future studies should consider the use of vignettes to improving our understanding of, as well as limiting participants' bias. Vignettes are descriptions of hypothetical situations and participants would be willing to be more open about their experience when these are used. The changing nature of the phenomenon under investigation in the current study renders the possibility of obtaining consistent results problematic due to the social constructive nature of real-world experiences. Because the work is context specific, the context will always be perceived to change. Notably, context always matters in qualitative research (Marshall & Rossman 2011). It is for this reason that the findings may not be readily generalisable. However, detailed processes described in the current study should enable other researchers to repeat the work; not necessarily be expected to achieve similar results (Lincoln & Guba 1985; Shenton 2004) but to determine how situations regarding computer failure would influence ISec behaviour.

11. Conclusion

The phenomenological study regarding understanding ISec behaviour that is shaped by various situational exigencies followed a structured and systematic approach. The study has provided a holistic understanding of how exigencies shape ISec behaviour. Exigencies denote the demands and pressures placed on employees during computer system failure situations, while computer system failure, with most of these exigencies explored from real-world experiences of employees. Underpinned by the philosophy of Husserl the study inductively collected qualitative data via in-depth, semi-structured interviews, from 12 employees (Husserl 1983). Data were analysed in two phases; firstly, via methods and procedures of phenomenological analysis and secondly via a summative analysis (Moustakas 1994). Exigencies are importantly highlighted as emotional constructs that cause a lot of frustration, when computer failure occurs. Other emotional constructs have been documented in the work as well. Aggregated results clearly show that the demands and pressures placed on employees during crisis resulting from computer system failure will influence ISec behaviour differently. This study shows that employee would exhibit intentional non-malicious ISec behaviour under these situations. We encourage future studies ISec studies to take cognisance of the exigencies of a situation when examining ISec behaviour. It is only by improving our understanding of employee ISec behaviour will organisations be able to deal with the emotions that will be presents when moments of crisis occur. We have presented insights on how may ISec practitioners may encourage mentally preparedness to avert emotional breakdown with these situations occur. Efforts should be made to ameliorate unwanted ISec behaviour resulting from highlighted exigencies in this work, by building on the foundations of the past, to lead us into the future of transforming the landscape of behavioural ISec research.

12. References

Andress J (2014) Chapter 1 - What is Information Security? *The Basics of Information Security (Second Edition)* (Syngress, Boston) 1-22.

Bamberger P (2008) From the editors beyond contextualization: using context theories to narrow the micro-macro gap in management research. *Academy of Management Journal* 51(5)(p.839-846.

Barrett C, Bisset K, Chandan S, *et al.* (2013) Planning and response in the aftermath of a large crisis: An agent-based informatics framework. *2013 Winter Simulations Conference (WSC)* (IEEE 1515-1526.

Barton L (2001) *Crisis in Organizations II*, (South-Western Cengage Learning).
Baumeister RF, Tice DM (1985) Toward a theory of situational structure. *Environment and Behavior, 17, 147–192.* 17(pp. 147–192.
Berger PL, Luckmann T (1966) *The Social Construction of Reality*, (Penguin books).
Bordens K, Abbott B (2010) *Research Design and Methods: A Process Approach*, 8th Ed. ed.(McGraw-Hill Medical Publishing).
Bowers KS (1973) Situationism in psychology: An analysis and a critique. *Psychological Review* 80(5):307-336.
Bryson JM (2004) What to do when stakeholders matter: Stakeholder identification analysis techniques. *Public Management Review* 6(pp. 21-53.
Candace LU (2009) Virtue Ethics and Moral Psychology: The Situationism Debate. *The Journal of Ethics*2(3)):pp. 103.
Cohn R, Carley KM, Harrald JR, *et al.* (2000) Emotions in crisis management: an analysis of the organisational response of two natural disasters. *International Journal of Technology Management* 19(3-5):313-335.
Coombs WT (1999) *Ongoing crisis communication: Planning, managing, and responding*, (Thousand Oaks, CA: Sage).
Crotty M (1998) *The Foundations of Social Research*, (SAGE Publications, Los Angeles).
D'Arcy J, Hovav A, Galletta D (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research* 20(1):79-98.
Darley J, Batson C (1973) From Jerusalem to Jericho: A study of situational and dispositional variables in helping behavior. *Journal of Personality and Social Psychology* 27(pp. 100–118.
Dean J (2007) Personality or Situation? The Psychology of Individual Differences. PSYBLOG.
Deutsch SE, Pew RW, Rogers WH, *et al.* (1994) Toward a Methodology for Defining Situation Awareness Requirements—A Progress Report. National Aeronautics and Space Administration, BBN Report, (7983).
Dowling M (2007) From Husserl to van Manen. A review of different phenomenological approaches. *International Journal of Nursing Studies* 44(1):131-142 112p.
Edwards JA, Templeton A (2005) The structure of perceived qualities of situations. *European Journal of Social Psychology* 35(pp. 705-723.
Firestone WA (1993) Alternative arguments for generalizing from data as applied to qualitative research. *Educational Researcher* 22 (1993)(pp. 16-23.
Francis JJ, Johnston M, Robertson C, *et al.* (2010) What is an adequate sample size? Operationalising data saturation for theory-driven interview studies. *Psychology & Health* 25(10)(pp. 1229-1245.
Funder DC (2006) Towards a resolution of the personality triad: Persons, situations, and behaviors. *Journal of Research in Personality* 40(1)(p. 21-34.
Funder DC, Colvin CR (1991) Explorations in behavioral consistency: Properties of persons, situations, and behaviors. *Journal of Personality and Social Psychology* 60(p. 773–794. .
Furr RM, Funder DC (2018) *Persons, situations, and person-situation interactions*).
Fusch PI, Ness LR (2015) Are we there yet? Data saturation in qualitative research. *Qualitative Report* 20(9)(pp. 1408-1416.
Giorgi A (1988) *Validity and reliability from a phenomenological perspective. In W. J. Baker, L. P. Mos, H. V. Rappard, & H. J. Stam (Eds.), Recent Trends in Theoretical Psychology*, (New York: Springer-Verlag).
Glaser BG, Strauss AL (1965) *Awareness of Dying*, (Aldine Publishing Company).
Gonzalez JJ, Sawicka A (2002) A framework for human factors in information security. In: *In: Paper presented at the World Scientific and Engineering Academy and Society (WSEAS), Rio de Janeiro*.
Guba EG (1981) Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Communication and Technology Journal* 29 (1981)(pp.75-91.
Guest G, Bunce A, Johnson L (2006) How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods* 18(pp. 59-82.

Guo KH (2013) Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* 32(242-251.

Guo KH, Yuan Y, Archer NP, *et al.* (2011) Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems* 28(2):203-236.

Herath T, Rao HR (2009) Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems* 18(2):106-125.

Hong W, Chan FKY, Thong JYL, *et al.* (2014) A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research* 25(1)(p.111-136.

Hu Q, Xu Z, Dinev T, *et al.* (2011) Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the acm* 54(6):54-60.

Huddleston R, Pullum GK (2002) *The cambridge grammar of english. Language.*, (Cambridge: Cambridge University Press, pp.1-23.).

Husserl E (1983) *Ideas Pertaining to a Pure Phenomenology and to a Phenomenological Philosophy*, (Martinus Nijhoff Publishers: The Hague.).

Ifinedo P (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31(1)(pp. 83-95.

Johns G (2006) The essential impact of context on organizational behavior. *Academy of Management Review* 31(2)(p.386-408.

Johnston AC, Warkentin M, M S (2015) An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioned Rhetoric. *MIS Quarterly* 30(1):113-134.

Kenrick DT, Funder DC (1988) Profiting from controversy: Lessons from the person-situation debate. *American Psychologist* 43(p. 23-34.

Lerbinger O (1997) *The crisis manager: Facing risk and responsibility*, (Mahwah, NJ: Erlbaum.).

Lincoln YS, Guba EG (1985) *Naturalistic inquiry*, (Beverly Hills: Sage).

Loch KD, Carr HH, Warkentin ME (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly* June(173-186.

Mack N, Woodsong C, Macqueen KM, *et al.* (2005) *Qualitative Research Methods: A Data Collector's Field Guide*, (Family Health International, North Carolina, USA).

Marshall C, Rossman GB (2011) *Designing Qualitative Reseach*, Fifth Edition ed.(SAGE Publications, Inc.).

Merriam-Webster.com (2020) "effective." https://www.merriam-webster.com (21 February 2020).

Meyer RD (2015) Taxonomy of Situations and Their Measurement. Oxford University Press, Oxford Handbooks Online.

Mischel W (1968) *Personality and assessment*, (Wiley).

Mischel W, Shoda Y (1995) A cognitive–affective system theory of personality: Reconceptualizing situations, dispositions, dynamics, and invariance in personality structure. *Psychological Review* 102(2)(p. 246-268.

Mishra S, Dhillon G (2006) Information systems security governance research: a behavioral perspective., Presented at 1st Annual Symposium on Information Assurance,

Academic Track of 9th Annual NYS Cyber Security Conference, 2006, New York, USA. In: *Presented at 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA*.

Moustakas C (1994) *Phenomenological research methods.*, (SAGE Publications, Inc., Thousand Oaks, CA).

Nisbett RE (1980) *Retrospections on social psychology*, (The trait construct in lay and professional psychology. In L. Festinger (Ed.), (pp. 109–130). New York: Oxford University Press).

Njenga K, Brown I (2012) Conceptualising improvisation in information systems security. *European journal of information systems* 21(6):592-607.

Paley J (1997) Husserl, phenomenology and nursing. *Journal of Advanced Nursing* 26(187-193.

Ponemon Institute (2017) Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview. Ponemon Institute LLC.

Pope C, Mays N (1995) Reaching the parts other methods cannot reach: an introduction to qualitative methods in health and health services research. *British Medical Journal* 311(6996)(pp. 42-45.

Rauthmann JF, Sherman RA, Funder DC (2015) Principles of situation research: Towards a better understanding of psychological situations. *European Journal of Personality* 29(pp. 363-381.

Ray MA (1994) *The richness of phenomenology: philosophic, theoretic, and methodologic concerns. In Critical Issues in Qualitative Research Methods (Morse J.M., ed.)*, (SAGE: Thousand Oaks).

Reiners GM (2012) Understanding the Differences between Husserl's (Descriptive) and Heidegger's (Interpretive) Phenomenological Research. *J Nurs Care 1:119*.

Ross L, Ward A (1995) Naive Realism: Implications for Social Conflict and Misunderstanding. *Stanford Center on Conflict and Negotiation, Stanford University*.

Safa NS, Ismail MA (2013) A customer loyalty formation model in electronic commerce. *Econ Model* 35(0)(pp. 559-649.

Safa NS, Sookhak M, Von Solms R, *et al.* (2015) Information security conscious care behaviour formation in organizations. *Computers & Security* 53(65-78.

Sarantakos S (2013) *Social research*, Fourth edition ed.(Palgrave Macmillan, UK).

Saumure K, Given LM (2008) *Data saturation.*, (Thousand Oaks, CA: Sage, In L. Given (Ed.), The SAGE encyclopedia of qualitative research methods).

Schneier B (2000) *Secrets and Lies: Digital Security in a Networked World*, (Indianapolis: Wiley Computer).

Shenton AK (2004) Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information* 22(2004)(pp.63-75.

Siponen M, Vance A (2010) Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3):487-502.

Siponen M, Willison R (2009) Information security management standards: problems and solutions. *Information and Management* 46(5)(pp. 267-270.

Son JY (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Inf Manag*.

Spiegelberg H (1971) *The Phenomenological Movement: A Historical Introduction, 2nd ed.* , (Martinus Hijhoff: The Hague.).

Tanggaard L (2009) The research interview as a dialogical context for the production of social life and personal narratives. *Qualitative Inquiry* 15(9)(pp. 1498-1515.

Thomson K-L, von Solms R (2006) Towards an Information Security Competence Maturity Model. *Computer Fraud & Security* 2006(5):11-15.

Van den Bergh M, Njenga K (2016) Information Security Policy Violation: The Triad of Internal Threat Agent Behaviors. *1st International Conference on the Internet, Cyber Security, and Information Systems (ICICIS)* (Department of Computer Science, University of Botswana, Gaborone).

van Manen M (1990) *Researching Lived Experience*, (The State University of New York Press, Ontario).

Vance A, Siponen M, Pahnila S (2012) Motivating IS security compliance: insights from habit and protection motivation theory. *Inf Manag* 49(190-198).

Workman M, Gathegi J (2007) Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology* 58(2)(212-222.

Zimbardo P (2007) *The Lucifer Effect*, (New York: The Random House).

Appendix

Participant	Researcher comments	Interviewee experience Regarding ISPs and role of IT in the organisation
Sakkie	• Familiar with ISPs because of attending a course. • Could not rely on IT Support to solve more complicated IT requests.	• 'I did a course somewhere and someone said I had to read that stuff' • 'I do think they make it clear. . . all the things in there are pretty clear' • 'My overall impression is, for the years that I have been here, they have always been helpful. I can't say anything bad about them' • 'But if you go into more detail IT stuff, like internal blocking of IP addresses. . . you can't really rely on them. But your normal day-to-day, desktop support from IT, is great. The more advanced IT stuff, I'd say is difficult to rely on'
Demi	• Familiar with ISPs and had recently read through them (because an incident occurred). • Perceives enforcement of ISPs as inconsistent. • Initial impression has changed over the years, specifically in relation to support for Macintosh computers.	• 'They (ISPs) are all on our intranet. I know they are, but whether I've read them or not, in 16 years. . . yes, I have actually. We had to punish somebody. . . recently, so I had to read through the security policies' • 'I find them inconsistent. . . . there are people that have found ways around it, and I just find that they are not punished for what they've done or found. . .' • 'In general, there wasn't much of an IT Support when I first started here. I think with the move toward Mac, the IT department kind of spruced-up their knowledge of Mac and what works on the network and what doesn't. They have some specialists now, so my impression of them has improved. It wasn't always great'
The Big Guy	• Wary of the organisation's ISPs and found them confusing. • Not sure where to find the ISPs and had only read these about two years back. • Services had improved over the years, particularly with respect to Macintosh support.	• 'I would say my overall impression is that it is all a bit confusing. I wouldn't even know that I'm violating policies. . .' • '. . . go to our portal, search somewhere under policies, and it's probably there somewhere. . .' • 'Every now and then we get a prompt to sign in, prompted due to changes to conditions or the policy. I've read the policy maybe 2 years ago. . .' • 'My overall impression is that they've improved their service levels quite significantly in the last year. . . Mac support. . . it's come a long way'

Charmaine	• Knew where to find the ISPs but had never read these. • Has never attended the organisation's induction programme. • Perceived IT Support as helpful (when calls were logged) but desk issues had a longer waiting time.	• '(ISPs) are all on [location withheld], which is our intranet. . .' • '[Have I] read any of them? Never. I also never did the induction process. I came in and started on projects. . . I've never been for an induction' • 'So, our helpdesk is twenty-four hours and they are really helpful and all of that. We do sometimes wait for quite a while for someone to come help you, which is frustrating because you'd be offline for quite a bit'
CO123	• Knew where to find these but perceived that the organisation's ISPs as only good on paper, with implementation challenging for IT support. • Perceived IT Support as having both positive and negative qualities and had improved on the technology they used as well as the quality of staff employed.	• 'These are (ISPs) very good. . . very good on paper. I know they are trying to implement a lot of ways to block people. There are a lot of sites that they do block you and you can't go into. . .' • 'Yes (know where to find them), we have a Web-based intranet. . . and all policies are there. . . haven't read any of them recently. . . There is something when you log in. . . a little pop-up and you would say that you have read through it, and you would accept, but a lot of people never read the document we just accept. . . just get it over and done with. . .' • 'In certain situations, it's (IT Support) perfect but there are definitely some problems. You can sometimes report a problem and then they don't know about it and then they can take forever to try and find the issue. . .' 'They have improved. . .'
RMAC	• Perceived ISPs as standardised and easy to comprehend. • Scant understanding of where to locate ISPs in the organisation and has not read them. • Not satisfied with the level of support obtained from IT personnel.	• 'They are quite straight forward. . . I think it's quite standard. I think it's sometimes a little bit over the top. . .' • 'The information security policies. . . on [location withheld] . . . I haven't looked. . . I'm sure that they are somewhere. . . I don't think the company does enough. . . in terms of the policies. . . Although they did towards the end of last year, they started taking us through. . . that sort of thing. . .' • ". . . is the first time in a while that I've said 'wow they have actually taken time to inform us about a specific policy'" • 'As employees we receive the lower level. . . of attention. . . That applies when IT [is] dealing with employees. . . From a [name withheld] experience, we definitely sort of given second rate support. . .'

Goldberg	• Perceived that great strides have been taken towards creating awareness amongst end-users from a culture where ISec used to be largely disregarded. • Many end users find difficulty in finding ISPs. • From an unstructured and lacking in IT governance, the IT support service has advanced.	• 'When I started working here, information security was a concept that was very easily kind of dismissed in line with governance controls. . .' • 'There wasn't an appreciation for the value of information security, largely because it's not a monetizable asset' • 'when we did an exercise to quantify the risk exposure of information. . . and that's when the senior management really started considering this' • 'I know where to find the policies, but not everyone does, that's unfortunately the reality in this place' • 'My perception of the IT department is it has evolved. When I started working here. . . our ITD was very unstructured. . . however, the perceptions have changed and evolved quite a bit'
Starlord	• Limited knowledge of ISPs but can at least find these. • Perceived limited enforcement of ISPs. • IT Support as generally acceptable particularly with Macintosh support.	• 'We've got a portal called [name withheld]. . . you have to go in and look for something if you curious. . . Nope I have not accessed the policies recently. . . to be honest my knowledge is actually quite limited on those information policies. . .' • 'In [organisation name withheld], it is not something that we are really made aware of. Not because they don't have them but because . . . and I don't think it is something that they actually really enforce' • '[My] general perception [of IT support is] mixed. I've had good experiences and I've had some frustrating experiences. . . especially because I'm a Mac user'
Mrs Philander	• Has not read ISPs and does not know where to find these. • IT Support is seen to be helpful although the time taken to resolve issues was considered long.	• 'There are a lot of emails that I don't read. . .' • 'No (I have not read any of the ISPs), I haven't done that. Unless they send it [to my email], I wouldn't necessarily read it. . .' • 'They've been helpful. . . sometimes it just takes a while for them to possibly understand the issue that I have. . . sometimes it takes a bit long. . .'

Mary	• Knowledge of where to find ISPs however, had not accessed these in the recent past. • Expressed disappointment regarding falling standards of IT Support.	• 'Yes [I know where to find the ISPs], on [name withheld] there is a place called 'Policies'. That is where I would look. . .' • 'I [have] not recently [read any of the ISPs]' • 'It's a bit mixed feelings. It seems in some ways to be deteriorating over time. . .' • 'I realise then that they are knowledgeable and aware of issues. So, I have a bit of confidence that there are people there who know what's going on, but I don't think they are always available to us when we call in with a problem. . .'
NodeCore	• Appreciated the value of ISPs and knew where to locate these although had not read them in the recent past. • Had been frustrated by the IT support services.	• 'I'd say they are good, in terms of protecting the IP, but also . . . very limited to certain frameworks and systems' • '[ISPs] are on the intranet portal. . . [name withheld] something like that. . . [I haven't accessed them], no' • 'No I haven't read them recently. Apparently, there are some that have changed, but I haven't read them in a while' • '. . . There is also a lot of frustration. Especially as a Mac user. . . competency may be there but as Mac users we feel like we are excluded basically from a whole lot of policies and procedures and admin related incidences. . .'
Grace	• Mostly uncertain regarding where ISPs were located and therefore had not read any of these. • Perceives that IT Support is overburdened compared to the requests made daily.	• 'I'm going to go with [name withheld] . . . but I highly doubt. . . I wouldn't be able to. . .' • It's going to be a no from me [I haven't read any of the ISPs recently]. You know, if I'm being honest, it is one of those things, it's like the Ts & Cs of iTunes. . .' '. . . I don't really think that there is any security. . . as far as people being able to come in and jump on and off our networks. . .' • 'I feel like, with the guys that I've dealt with, a lot of the time I get a sense [they are] being overstretched, because, like on our side, I can show you the guy that works this whole building. . .'