The African Journal of Information Systems

Volume 8 | Issue 1 Article 3

2016

We Want To Do It Our Way: The Neutralisation Approach to Managing Information Systems Security by Small Businesses

Kennedy Njenga
University of Johannesburg, knjenga@uj.ac.za

Pierre Jordaan
University of Johannesburg, Pierre.Jordaan@kpmg.co.za

The African Journal of Information Systems

We Want To Do It Our Way: The Neutralization Approach to Managing Information Systems Security by Small Businesses

Research Paper

Volume 8, Issue 1, January 2016, ISSN 1936-0282

Kennedy Njenga
University of Johannesburg
knjenga@uj.ac.za

Pierre Jordaan
University of Johannesburg
Pierre.Jordaan@kpmg.co.za

(*Received January 2015, accepted August 2015*)

ABSTRACT

Small businesses thrive in the developing economy of South Africa and address the important issue of unemployment and poverty that exists in the country. A large number of these businesses can be found in the province of Gauteng due to the large and diverse economic contribution the province delivers to the economy of South Africa. With the increased use of Information Systems (IS) by small businesses across the Gauteng province and in South Africa generally, there is increasingly constant exposure to information security risks. Interestingly, standards such as NISTIR 7621, specifically tailored to small businesses and which could offer great insights on how to manage security risks, are by and large not followed to the letter. We find in our work that owners-managers prefer to handle matters of security 'in their own terms' and apply neutralization (termed rationalization) techniques to overcome the effects posed by security threats. We used four instrumental cases for this purpose. Our findings suggest that neutralization manifests as values held by owners-managers and this can often create the unintended consequences of exacerbating security risk to these small businesses.

Keywords

Information Systems Security, Small businesses, Neutralization

INTRODUCTION

Small businesses thrive in the developing economy of South Africa and address the important issue of unemployment and poverty that exists in the country. The South African National Small Business Act 102 of 1996 identifies a small business organization as an *entity* that can either be legally registered or not registered and is mainly focused on conducting *small business matters*. If a small business is formally registered it would be likely that it employs more than five people but less than 100, and will have a fixed business premises (Gauteng

provincial government, 2010:7-8). A large number of small business organizations can be found in the province of Gauteng owing to the large and diverse economic contribution the province delivers to the economy of South Africa. Gauteng currently represents only 1.4% of South Africa's surface area but hosts around 23.7% of the country's population, which is close to 12.2 million people (SouthAfrica.info, 2012).

According to Stats SA's census report (Stats SA, 2012), small businesses operate in Gauteng's three metropolitan municipalities namely: city of Johannesburg, city of Tshwane and Ekurhuleni Metro, as well as two district municipalities, namely: Sedibeng and the West Rand. These municipalities hold the following unemployment rates as shown in Table 1 below.

***Table 1**: Summary of Districts in Gauteng Province, South Africa (Stats SA, 2012)*

Municipality	**Type**	**Unemployment Rate 2011**
City of Johannesburg	metropolitan	24.7% Unemployed
City of Tshwane	metropolitan	24.2% Unemployed
Ekurhuleni Metro	metropolitan	28.8% Unemployed
Sedibeng	district	32.0% Unemployed
West Rand	district	26.7% Unemployed

Between the periods of 1985 and 2005, only around 10% of the employment opportunities were created by large established firms, showing the need to focus on the growth of small businesses (SBP, 2009). In a study conducted on small businesses in the USA, it was found that information technology could leverage the success of a small business, through better services to the customer and also executing business processes more efficiently (Beheshti, 2004). Within the small business environment, information technology has been known to "*increase business efficiency and benefits as well as to make the organization more competitive towards the outside business environment*" (Baard and van den Berg, 2004).

Because of the increased cheaper broadband rates, (Grobler and Jansen van Vuuren, 2010) as well as affordability of information systems (IS) technologies, many small South African businesses are incorporating the use of information systems as part of their core processes (Carkenord, 2009). This traction in IS diffusion has therefore resulted in many small South African businesses increasingly becoming dependent on the use of IS. A crucial concern is that the use of IS is coupled with inherent information and cyber-security risks that many small businesses might not be aware of.

Many small South African businesses lack the proper mechanisms to control emergent cyber-security risks and information systems security threats that characterize the use of these technologies. This concern has been raised by researchers such as Grobler *et al (2011:113)* who describe the digital space as a "*dangerous place that poses a threat to the local community*" of South Africa. This knowledge is of great importance to researchers and small businesses particularly towards understanding how risks are managed by owners-managers.

Since owners-managers are the primary decision makers on all matters pertaining to the day-to-day management and running of the small businesses, it follows then than a deeper insight

on how they manage cyber-security risks is required. We note that the decision making processes can often give rise to information security concerns because such decisions may cause intentional or accidental security risks to these small businesses (D'Arcy, Hovav and Galletta, 2009; Im and Baskerville 2005).

Frameworks for the right decision making process

Often the right decisions to be made by those who manage small businesses should be steered by standards, policies and guidelines that would effectively make information more secure and cyber-security risks less of a threat in these small businesses. Some of the decisions to be made are (Yildirim *et. al.*, 2011):

- acceptable security levels for user accounts
- frequency of passwords changing
- password complexity
- backing-up data
- access privileges
- confidentiality of information

Small businesses in South Africa are endowed with a few global standards, policies and guidelines that would allow these small businesses to reinforce correct decisions such as the above listed. The British Standard (BS) 7799, the ISO/IEC 17799 and Chapter XIII of the Electronic Communications and Transactions (ECT) Act of South Africa are the most widely used of these standards (Bougaardt and Kyobe, 2011). The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has also set up minimum provisions to be followed by small businesses towards effecting proper controls over use of technology. In 2013, COSO updated and issued the *Internal Control—Integrated Framework* which stipulates basic components of internal control that should be present in small businesses (McNally, 2013). The National Institute of Standards and Technology (NIST) has equally issued a guide specifically for small businesses to help them in their planning for security. The NIST Interagency Report (NISTIR) 7621, *Small Business Information Security: The Fundamentals*, presents areas that small businesses should cover for their information systems (Heier, 2014).

We contend that while the standards, policies and guidelines might be easily available, not many small businesses are keen to follow these to the letter. Anecdotes suggest that many owners-managers of small businesses rationalize why they would consciously disregard these good tenets. This assertiveness can be termed neutralization and the next section elaborates on this aspect further.

Neutralization

Li, Zhu and Pan (2012) have expressed concern that owners-managers of small businesses lack enough skills to make the right decisions particularly in situations where problems occur. They postulate that, most decisions made are subjective and are inherently biased. To cope with emergent security threats that constantly affect the security of small businesses the owners-managers will at times apply neutralization (termed rationalization) techniques that assists in decision making. Neutralization theory proposes that individuals will rationalize their decisions as acceptable and 'ok', irrespective of whether or not these decisions are compliant with standards and guidelines (Sykes and Matza, 1957). Of concern to practitioners of information security is that when owners-managers apply neutralization techniques and rationalize on wrong decisions, these decisions might tend to intensify rather than mitigate against information and cyber-security risks (Barlow, Warkentin, Ormond and Dennis, 2013).

Research problem
Little is known about how neutralization techniques as operated by owners-managers of South African small businesses are manifested. Little is also ~~is~~ known about the extent to which these neutralization techniques and by extension standards, policies and guidelines are adhered to. This work aims at filling this gap in literature by considering the impact neutralization has on the security posture of small businesses in South Africa. The work specifically applies concepts from the NIST Interagency Report (NISTIR) 7621, *Small Business Information Security: The Fundamentals*, to conceptualize neutralization in these small businesses.

Research questions
The objective of this research work is therefore to provide deep insights regarding how the techniques of neutralization are used as decision-making aids by small businesses owners-managers in South Africa. In addressing the research objectives, the following are explicit research questions that provide clarity on the research work:

1. how is neutralization manifested and made evident when owners-managers of small businesses in Gauteng South Africa manage cyber-security threats?
2. how does neutralization impact the security posture of these small businesses?
3. how would neutralization be addressed in these contexts so that owners-managers are better suited to manage cyber-security threats more effectively?

In an attempt to answer the above questions, we take a qualitative approach and focus on four cases that were ideally selected because of the rich qualitative data that these cases offer. We qualitatively examined the *National Institute of Standards and Technology Interagency Report (NISTIR) 7621 for Small Businesses* to understand how such a standard would be neutralized by small businesses.

The rest of the sections are structured as follows:
the next section describes emergent cyber-security threats to small businesses and outlines behavioral concerns espoused by owners-managers. What follows is a conceptual discourse around the phenomenon of neutralization and its perceived influence on decision making in small businesses. The theme is predominantly decisions made by owners-managers on the need to mitigate against information systems security threats. The penultimate sections consider the methodology used to obtain data, how this data was analyzed and finally a discussion regarding findings is presented. The concluding section explains what these findings mean to small businesses operating in South Africa.

CYBER-SECURITY THREATS TO SMALL BUSINESSES

Idrach (2011) has raised the question on whether small business'owners-managers have the right attitude towards security. This is important considering that many small businesses do not align security needs to business goals (Sangani, *et al*., 2012). Small businesses therefore become exposed to threats and software vulnerabilities such as computer virus, malware, phishing attacks and hacking that have a heavy financial bearing (Sangani, *et al*., 2012). The main concern is that small businesses are largely dependent on information technology investments which assist them to enhance and grow their business. Furthermore, while many are keen to rush and utilize these emergent technologies, these small businesses often lack the

necessary skills and awareness regarding standard procedures for mitigating information security risks. Many small businesses do not necessarily understand risks and consequences that may lead to security risks, and resulting financial implications (Idrach, 2011).

Many small businesses fail to consider information security because of a number of reasons that include: "limited budget, limited time to invest in training and awareness, little appreciation for risk and fewer compliance drivers", Idrach, (2011:19). Information security *awareness* from a small business owner-manager's perspective often describes a condition where the owner-manager recognizes the importance of information security as well as the role they play in ensuring that information as a business asset is kept safe (Boucher and Flowerday, 2011:2). Gaining knowledge and awareness regarding information security threats is largely driven by the need to protect information systems and knowledge assets against cyber-criminals.

In developing countries contexts, cyber-crimes and information systems risks have a greater impact on business existence and survival, and is commonly seen as the result of a lack of "*law enforcement and expertise*" (Salifu, 2008:440). Furnell, Gennatou and Dowland (2002:352) note that information security is "*critical*" to "*businesses that are technology dependent*" and conclude that this understanding is notably "*lacking in small business organizations*". While the lack of awareness about information security concerns especially by small businesses may be a global problem, the effects are more pronounced in developing countries such as South Africa (Salifu, 2008). In Gauteng, South Africa for instance, small businesses lack the proper mechanisms to understand appropriate technologies such as "*antivirus or firewall software*" and the possible cyber threats that exist. These businesses encounter challenges when it comes to selecting the right technical security solutions from the market because they lack the financial and/or technical capacity "*to employ someone that has a professional knowledge on cyber security*" (Bhattacharya, 2011:302). Typically, many small businesses have few if any at all IT professionals who manage~~s~~ the entire setup (hardware, software and network needs) of the small business. According to Bhattacharya (2011) many of these small businesses end up outsourcing most if ~~it~~ not all of their security needs.

In a study focusing on small IS dependent businesses~~;~~ , it was observed that awareness levels were raised only through "*an environment where mistakes were made and lessons learned*" (Furnell *et al*., 2002:354). Further studies on the small business environment of South Africa indicated that many had not adopted formal information security and awareness frameworks as well as frameworks that deal with privacy and protection of personal identifiable information (Upfold and Sewry, 2005). Additionally, many of these businesses were not even aware that these threats existed (Perks, 2010). Since security and privacy had not been the prime concern of many small businesses, many were operating under the notion that by just installing an anti-virus software "[*the software] would take care of all security threats*" (Sangani and Vijayakumar, 2012). With such lack of awareness and training levels noted, it is surprising that many small businesses still flourish amidst emergent and often turbulent cyber environments. The next section discusses how lack of awareness regarding security matters is an antecedent to neutralizs~~s~~ation.

Neutralization and bounded values

Although, it can be agreed that owners-managers are actively involved in the day-to-day management of small businesses in Gauteng, there is an increasing need for these to perform security related decisions such as installing anti-virus software, avoiding questionable emails

(phishing emails) and encouraging the use of strong passwords in their small businesses (Barlow, *et al.,* 2013). Results from a South African study emphasized the need for the presence of information security awareness in business organizations as well as the importance of a '*localized approach'* to the needs of the business (Thomson, 2008).

The greatest threat regarding security in small businesses is the owners-managers and the security decisions they make (Warkentin and Willison, 2009). Small businesses would be exposed to security risks if owners-managers made security related decisions that are accidental or out of volition causing threat to data. This can be rationalized (termed neutralization) for instance when they perceive security procedures as hindrance to their job performance. Neutralization techniques as elements of cognition would be employed to rationalize non-compliance of policy with statements such as "*we really don't need strong passwords, we are a small company*". Indeed negligence in security compliance represents over 40% of information security related incidents in the U.S. and U.K. (Ponemon Institute, 2013).

The theory of neutralization techniques which originated from psychology studies considers several types of neutralization (rationalization) that explains non-compliant decisions (Sykes and Matza, 1957). Neutralization has been applied in information systems security policy research by Siponen and Vance (2010). Studies confirm that neutralization is an important predictor to non-compliance (Warkentin and Willison, 2009). According to D'Archy *et al*., (2009), lack of awareness has been shown to be an important measure towards increasing non-compliance regarding security. It should be noted that the non-compliance would be an outcome of lack of awareness and not necessarily by choice.

We consider that neutralization is more often than not the primary cause of non-compliance or '*costly mistakes'* in security matters by small businesses. It follows therefore that our research was an attempt to understand awareness (or lack thereof), and how this influenced the kinds of neutralization techniques employed by owner-managers of small businesses across Gauteng province in South Africa. The next section elaborates on the method used to understand the phenomenon of neutralization in small businesses across Gauteng, South Africa.

METHODOLOGY

In order to understand the phenomenon of neutralization in small businesses across Gauteng, South Africa we used a qualitative research approach. Qualitative research works towards "*describing the quality of a phenomenon*" (such as in our case, neutralization) instead of necessarily answering questions regarding the phenomenon statistically and numerically (Blumberg *et al.,* 2008:192). Qualitative management research is difficult to define in a single manner and has to be specifically tailored to its intended research environment (Johnson, Buehring, Cassell and Symon, 2007:37).

The benefit of a qualitative research approach to this work is twofold:
-first, it will allow the researchers to "*see and understand the context within which decisions and actions take place*" (Myers, 2013:5),
-second, it provides an opportunity for practice to gain insights on the relatively newness of the "*sociological and psychological*" aspects of neutralization within small businesses (Blumberg *et al*., 2008:192). One feature of the qualitative approach that the researchers also

found important is that this approach constituted an empirical investigation that had to primarily rely on empirical data from the social world.

We contend that it would have been impossible to understand why owners-managers of small businesses did what they did and why something happened without first talking to them and obtaining empirical data (Myers, 2013). According to Myers (2013), qualitative research in this instance would have been the best approach to use since we would be researching the phenomenon of neutralizsation in-depth. It is for this reason that we studied four organizations that were dependent on IS within the Gauteng region in South Africa where neutralization would be studied in context. These four cases were selected because of the rich insights each would yield. The interpretivism stance was adopted in order to understand "*meaning and the individualized ways of living by owners-mangers"* (Beck, 1992). The use of subjectivism and interpretivism fit well with the qualitative research study.

Case selection

Using criterion based, critical case sampling, (Turner, 2010:757) we first developed an instrument called the '*Information-Technology-Dependency tool'* which was distributed across ten randomly selected businesses. Small businesses owners-managers were asked (using structured questionnaires) how dependent they were regarding the use of IT solutions and how IT was supporting core processes (Blumberg *et al*., 2008:253). This criterion then informed us on the choice of determining the most appropriate case. We narrowed down to four cases that adhered to the set criterion (Saunders *et al*., 2009:240).

Procedure

Non-standardized, semi-structured interviews were used to gather the primary empirical data. This was useful in helping the interviewees '*to stay on topic'* (Saunders *et al*., 2009:360-371). During these interviews, we made use of techniques such as the Kruger, Drevin and Steyn, (2010) "*vocabulary test*" or "*consensus ranking*", which enabled the understanding of information security awareness of interviewees and the phenomenon of neutralization. Data from the interviews enabled us to prioritize the different aspects of information security awareness exhibited by owners-managers of small-businesses (Kruger and Kearney, 2008:255). The most relevant IT person in the small business (mostly identified as the owner-manager) was selected for the interview (Tsohou, Kokolakis, Karyda and Kiountouzis, 2008:330). The themes identified for interviews (drawn from the literature review) included the interviewees understanding and mitigating security efforts regarding

(i) security of information and technology as part of the business and access controls,
(ii) information and technology failures resulting from poor back-up procedures,
(iii) complexity of passwords,
(iv) control of personal information and phishing emails, and finally,
(v), anti-virus, and anti-malware solutions existing in their small business.

Background Cases

Organization 1: *Finance and Business services*

This organization specializes in offering payroll and tax-related services to small businesses. Organization 1 is based on a partnership business structure. The organization has six permanent employees and two other employees on a contract basis. The co-owners of this small business organization indicated that the organization makes use of information technology on a regular basis and is heavily dependent on IT for core processes. When describing its everyday business processes and activities, it was noted that IT forms a large part of the company and how it makes its revenue. The two business partners that co-own this organization were interviewed.

Organization 2: *Retail and Motor Trade and Repair services*
This organization specializes in the trade and repair of second-hand vehicles and is a leader within its operating market in Gauteng. The business has a single owner along with a number of management staff. Organization 2 employs around 45- 50 workers, which classifies it as a small business according to the National Small Business Act of 1996. An analysis of data generated from the IT-dependency tool confirmed that this specific organization made use of IT regularly. The analysis further confirmed that IT has created competitive advantage for the business. The small business owner-manager was interviewed.

Organization 3: *Finance and business services*
Organization 3 is a small auditing firm that has a relatively large client base in the Gauteng province. The organization generates and makes use of personal and sensitive information on a daily basis. An analysis of the IT-dependency tool confirmed dependency on IT for core processes within this small business. The processing of financial, tax and other personal and sensitive information was done using technology systems and this formed part of the daily business activities. Both the partner and owner of the auditing firm were interviewed.

Organization 4: *Finance and business services*
This organization employs 15 people and operates in the advertising industry of Gauteng, as well as the rest of Africa. The senior manager of the small organization suggested that IT was incorporated into daily operations particularly in market research. Some of the services rendered by this small business were anchored on e-commerce technology with a sizable number of other business processes being supported by integrated network technologies. It was also noted that a big portion of the small business revenue was earned through technology based operations that included e-commerce and online advertising. The senior manager, who reports directly to the owner of the business~~,~~ was interviewed.

Narrative: IS/IT dependency
Interviewees from the four cases selected from Gauteng, South Africa confirmed the use of common operating systems and software applications such as *Microsoft*™ and *Microsoft Office™* related products within their small businesses. *Pastel*™ was the most commonly mentioned software package used by these small organizsations. Two interviewees mentioned *VIP*™ as the preferred payroll solution. An interviewee from organizsation 1 explained that *Pastell*™ and *VIP Payroll*™ were used in conjunction with online banking applications. The interviewee from organization 3 confirmed that their small organization used accounting *Caseware*™, *Pastel*™ and *Pastel Payroll*™. Outside of the reliance of vendor-based software, an interviewee from organization 2 specified that their small organization also made use of customized software applications that were tailored to their own specific business needs. Both interviewees from organizations 2 and 4 also confirmed the use of *Microsoft*™ and *Pastell*™.

The interviewee (owner-manager) from organization 2 expressed the dependency of this tailored software:

> "*Software that is specifically written in-house [means] everything [to us]*!"
> *"Our entire business is dependent on information technology! From sales to marketing to client communications."*

The interviewees were unanimous that information technology had brought changes to how they ordinarily run their businesses. Asked whether they supported these changes, the interviewees affirmed:

> *"yes definitely";* and
> *"we really support the change information technology brings to the business."*

Interviewees also expressed concern that such dependency and use of technology also brought unintended consequences, such as disruptions, data integration and/or interoperability issues. An interviewee from organization 1 illustrated one such process failure as being attributed to a 'compatibility' issue that was not anticipated:

> *"…exactly what happened today… I will introduce a certain program and maybe it's a newer version and then it's not compatible to old versions…."*

Narrative: How Neutralization was occurring

An interviewee from organization 2 gave the example of a backup that was not made for two months, and when a failure occurred, the small business lost two months of work. The failure and loss of business information was devastating to the organization with the interviewee (business owner) stating that the business had not been able to fully recover since that occurrence. Some of the interviewees' responses were as follows:

> *"I don't want to tell you how much two months is in this company! We service over 300 cars a month. It was a nightmare!"*

> *"I lost everything! [I'll] never be able to catch-up on everything…!"*

The interviewee described a scenario where a failure in business IT happened because of an accidental damage to the backup disk. This was brought about by careless handling, as explained below:

> *"My clerk dropped [the] back up [disk]! Now I cannot restore it and the data is lost!"*

The loss of information caused disruption to the business. The interviewee (owner-manager) further explained how this lost information was crucial to the trading and repairing of motor vehicles. Dependency of information technology in the small business was again emphasized in this instance.

We observed that these small organizations were primarily dependent on third parties such as banks to provide assurance and guarantees on matters pertaining to information security. There wasn't any observable indication that these small organizations were proactive in the security of information. An interviewee from organization 1 explained that they were satisfied with the way the online banking authentication codes were changed on a monthly basis:

> *"Our codes change every month, you change your codes and there is two sets of codes to change, and there is approval that you have to do."*

One way of avoiding the responsibility of securing their systems when using the internet for online banking transactions, as explained by an interviewee from organization 3, was that of restricting the online banking process or doing away with it entirely:

> *" restricting access to the online banking [because] enough comfort exists over the possible risks".*

On matters pertaining to phishing threats, one of the interviewees (co-owner) from organization 1 gave a specific example of a phishing related request that the small business had experienced in the past. The participant acknowledged not responding to this specific request, since this was identified as not being genuine. The interviewee explained:

> *"I received one this week from somebody stating [that] you must reply and contact the bank because there is a check paid into your account [which] has not been cleared. I went into my bank account and saw that there is no other money that I know about..."*

The interviewee from organization 2 (owner) explained that he occasionally enforced awareness amongst his employees on matters pertaining to phishing:

> *"If I get something like that I remind the employees not to respond…"*

An interviewee from organization 1 confirmed that employees were made aware of the dangers of phishing emails. However, this, as he seemed to suggest, was made verbally:

> *"I just said to them, ignore it!"*

Interestingly, interviewees from organizations 4 and 5 suggested that they were unaware of policies that existed in their organizations on mitigating against risks of phishing. An interviewee from organization 3 pointed this out. Prodded on the dangers of phishing, the interviewee's response was:

> *"If the employees click on the links [on the email], it's their own problems. Then it would be their work that is affected…I haven't spoken to them about it and if they are stupid enough to fall for it they have to learn from it..."*

An interviewee from organization 3 confirmed that business and customer information was stored on any available device including individual laptops, backup drives, hard-copy files and other information storage mediums:

> *"There is no specific place, it's mostly company information and we store it everywhere."*

The same interviewee (organization 3 owner) also stated that the small business had restricted access to hard-copy personal and sensitive information. Such information was kept locked in filing cabinets. Conversely, electronically available information was accessible to all the employees~~.~~ :

> *"…everybody has access to the information…the business is so small so everybody that works here [and needs] the information every day [gets it]… In a bigger business*

> *I guess there would be a risk… personal information of the employees is stored in my office..."*

An interviewee from organization 3 even suggested that they do not enforce access and confidentiality policies. When queried about slackness in attitude towards controls, an employee from-organization 1 responded:

> *"We started with passwords on individual computers, but I asked them to remove them because it's just a nuisance."*

Interviewees from organizations 1, 2 and 3 confirmed that access to servers they had was restricted by passwords. Interestingly, only one of the small organizations sampled consistently enforced the use of passwords on employee computers.

On matters concerning the use of illegal and unauthorized software use, an interviewee from organization 2 suggested an interesting approach he employed to deter this practice:

> *"We have nothing as such! I'll […] someone if he does that."*

This interviewee acknowledged having certain blind-spots concerning activities his employees performed on their work computers:

> *"…If you ask me… if my employees are doing things on their computers, how would I know? I don't always look at their things; I don't know what they do on their computers… I'm sure if they are downloading illegal stuff my IT-guy would pick it up..."*

Most interviewees claimed to have legal up-to-date software, with the exception of the interviewee from organization 3 (owner) who revealed that the software they used on the premise had in fact expired:

> *"Yes [we have] but it's outdated. Mine is expired and I have to get it updated."*

It was interesting that although the small organization was using an expired software, this did not seem to constitute such a big deal for the owner.

Matters concerning physical security of organizations' assets were also raised. When one interviewee from organization 2 was asked whether an encounter on physical security breaches had ever been experienced, the owner-manager responded:

> *"…we've been lucky; no one has ever broken in and stolen our computers and other equipment."*

> *"…we are extremely lucky..."*

The owner-manager confirmed that while, there had never been a known incident regarding the theft of information technology, the small business did not necessarily feel that it was adequately protected.

Based on this narrative data, we embarked on a deeper analysis using formally established analysis and coding methods. The next section elaborates on how we coded and interpreted the above narratives.

Coding

Elements on the above narratives "*identified as meaningful*" were coded for deeper meaning by "*a reconstruction of life's construction*" (Harper, 1998). We recorded the direct quotes (*verbatim*) and ascribed them numbers. We then analyzed the rationalization and meaning behind what was said by owners-managers. This was also recorded. We examined these comments against established security tenets in an attempt to assess underlying awareness levels that these owners-managers presented. We thoughtfully consider these comments to in an attempt to understand neutralization as a technique used towards mitigating security threats. We used the sequence of understanding of neutralization as described by Denzin (1989:46) as follows:

(i) securing the interactional text (that exemplified neutralisation)
(ii) displaying the text as unit
(iii) subdividing the text into key experiential units
(iv) linguistic and interpretive analysis of each unit
(v) serial unfolding and interpretation of meaning of the text to participants
(vi) development of working interpretation
(vii) confirming meaning against text
(viii) grasping text as a totality
(ix) displaying multiple interpretation that occur within text.

By following Denzin (1989) procedure for interpretations we highlighted the most significant problem representation/framing that was acutely different from acceptable treatment of security, and flagged these as '*experiential units*' to be considered. We established over 75 experiential units. The experiential units (***which best exemplified neutralization***) were risk assessed and mapped against the following risk elements:

(i) *impact to profits,*
(ii) impact to reputation,
(iii) impact to litigation, and
(iv) impact to business continuity.

We present the selected experiential units and interpretation shown by **Table 2** below.

***Table 2**: Interpretation of Experiential Units of Neutralization by owner-managers of small businesses*

Experiential unit #	**Rationalization :** *Text subdivided as key experiential unit (Denzin, 1989)*	**Security tenet to have been followed**	**Neutralization by owner-manager:** *What was actuality done*	**Researcher's Memo:** Development of working interpretation					
				Interpretation	**Risk Measure** *E = Extreme Risk* *H = High Risk* *M= Moderate Risk* *L = Low risk*	Impact to Profits	Impact to Reputation	Impact to Litigation	Impact to Business continuity
#23 #25	*"I lost everything! [I'll] never be able to catch-up on everything!"* *"My clerk dropped [the] back up [disk]! Now I cannot restore and the data is lost!"*	**Regular Back-up**	*Decided not to back up*	*Lack of proper disaster recovery procedures and business continuity procedures* ***Section 2.5* of NISTIR 7621**	**E**	✓	✓	✓	✓
#31 #33	*"Our codes [passwords] change every month, you change your codes [passwords] and there is two sets of codes [passwords] to change, and there is approval that you have to do."* *"We started with passwords on individual computers, but I asked them to remove it because it's just a nuisance."*	**Ensure Password complexity**	*Decided that Passwords and approvals were disruptive*	*Lack of standard access control procedures* ***Section 2.9* of NISTIR 7621**	**M**	✓	✓		
# 38	*"We [are] restricting access to the online banking"; [*because] *enough comfort exists over the possible risks".*	**Ensure Secure Online banking**	*Decided to eliminate this process altogether*	*Lack of online banking preparedness* **Section 3.4 of NISTIR 7621**	**M**	✓			

Experiential unit #	**Rationalization :** *Text subdivided as key experiential unit (Denzin, 1989)*	**Security tenet to have been followed**	**Neutralization by owner-manager:** *What was actuality done*	**Researcher's Memo:** Development of working interpretation					
				Interpretation	**Risk Measure** *E = Extreme Risk* *H = High Risk* *M= Moderate Risk* *L = Low risk*	Impact to Profits	Impact to Reputation	Impact to Litigation	Impact to Business continuity
#52 #56	*"If the employees click on the links [on the email], it's their own problems. Then it would be their work that is affected."* *"I haven't spoken to them about it and if they are stupid enough to fall for it they have to learn from it."*	**Develop Policy on Phishing**	*Decided to eliminate this process altogether*	*Lack of an effect policy creates poor framing / representation of problem for phishing* **Section 2.8,3.1 of NISTIR 7621**	**H**		✓	✓	
#59 #60	*"There is no specific place, it's mostly company information and we store it everywhere."* *"…In a bigger business I guess there would be a risk… personal information of the employees is stored in my office..."*	**Develop Policy regarding storing of personal data**	No specified policy	*Lack of awareness results poor framing / representation of problem* **Section 2.10 of NISTIR 7621**	**H**	✓	✓	✓	
#66	*"…everybody has access to the information…the business is so small so everybody that works here [and needs] the information every day [gets it]…*	**Develop categories of Information Access control**	The lack of classification on information access control	*Lack of awareness results poor framing / representation of problem* **Section 2.6 of NISTIR 7621**	**H**	✓	✓	✓	

We used *ATLAS.ti*™ software to establish the major concerns (*concepts derived from selected experiential units*) that faced owners-managers of small businesses when they tackled information security issued. By using a hermeneutical interpretative approach, we established six key themes, categorized from experiential units that were the essential components for understanding neutralization of well understood security tenets. They were *back-up of data, password complexity, online banking, policy on phishing, storage of personal data* and *access control.*

DISCUSSION AND RESEARCHERS INTERPRETATION: 'WHY WE WANT TO DO IT OUT WAY'

The interpretation is structured on the six themes outlined above. The six themes are interpreted using NISTIR 7621 as a guide and in accordance to what Barrett and Walsham (2004) cite as 'positioning as translating interests'. This means that the interpretive work could make a contribution if there is acceptance of our knowledge claims on neutralization. The basis of our interpretation is our assumption that owners-managers were creating and associating their own subjective meaning of security of systems unaware of what NISTIR 6721 was suggesting (Walsham, 1995). Therefore, we embarked on a deep and systematic interpretation of the six themes using NISTIR 6721 so that the insights produced by the interpretation in each theme could be generalized (Walsham 1995).

The interpretation section that follows attempts to answer the first *research question* regarding how neutralization is manifested and made evident when owners-managers of small businesses in Gauteng South Africa address cyber-security threats. It also explains in the following paragraph the impact of neutralization on the security posture of these small businesses which was *the second research question.*

Back-up and Storage

The issue of backing up data is closely related to how well small businesses plan for and survive during times of disaster. We observed deficiencies in planning for such an event. The following statement supports this:

> *"I lost everything! [I'll] never be able to catch-up on everything!"* and *"My clerk dropped [the] back up [disk]! Now I cannot restore it and the data is lost!"*

Researchers' interpretation regarding Back-up and Storage

Section 2.5 of the NISTIR 7621, recommends that it is essential that small businesses back-up data on each computer used in the business. It was clear that from the cases selected, not much importance was attached to this procedure. It might have been that the probability of a disaster such as this happening [losing of data] was minimal and this expectation tended to neutralize the need to back-up data as recommended. In terms of appropriating a measure for risk we interpreted and assigned this neutralization as **E = *extreme risk***. This is shown by **Table 2** above. This means the adopted neutralization would possibly have a big impact to profits, to reputation, to litigation and to business continuity.

Password use and complexity
When the use of passwords in small businesses was considered, neutralization manifested with statements such as:

> "*We started with passwords on individual computers, but I asked them to remove it because it's just a nuisance."*

Researchers' interpretation regarding Password use and complexity
Section 2.9 of the NISTIR 7621 recommends the use of passwords in small businesses as an "*absolute necessity*". The standard proposes that each small business should "*set up a separate account for each individual and require that good passwords be used for each account*". It further recommends that good passwords should consist *"of a random sequence of letters, numbers, and special characters and at least 8 characters long*". The standard asserts that employees should not have administrative accounts.

Our interpretation is that the owners-managers neutralized this requirement by requesting passwords to be removed from this specific organization, this created risk to the small business. In terms of appropriating a measure for risk, we interpreted and assigned this neutralization as M = ***moderate risk***. This is shown by **Table 2** above. This means the adopted neutralization may have a moderate impact to profits and to reputation.

Secure Online Banking
We noted that small business owners had an inconsistent understanding of security threats when using online banking. The belief that there were '*no risk concerns'* was dominant. There was no indication that the small businesses were proactive in addressing their own security needs. An interviewee from **case 1** explained that they were content with the way the online banking authentication codes (passwords) were changed on a monthly basis:

> *"We [are] restricting access to the online banking" [because] enough comfort exists over the possible risks".*

Researchers' interpretation regarding Online Banking
NISTIR 7621 *section 3.4* has issued provisions on the best way that small businesses can conduct online business and banking more securely. This section stipulates that it is necessary for small businesses to use a secure browser connection (indicated by a small lock visible on the lower corner of web browser). It also recommends that the "*web browser cache, temporary Internet files, cookies, and history associated with online commerce or banking sessions should be erased after the end of the sessions* (p. 9)". This would *"prevent sensitive information from being stolen by a hacker or by a malware program, if the system has been compromised"*.

To the small businesses, it was more convenient to "*restrict access to the online banking",* entirely than to appropriate the necessary controls. This neutralization effectively shut down and eliminated such a process altogether. This showed a lack of online banking preparedness. Our interpretation for this neutralization was that although shutting down the entire process seemed to have been rationalized as a less risky approach, small businesses were deprived of the opportunity to benefit from the advantages such a technology yields. In terms of appropriating a measure for risk we interpreted and assigned this

neutralization as L **= *Low risk***, this is shown by **Table 2** above. This means the adopted neutralization will have a moderate impact on profits.

Phishing

Owners-managers neutralized phishing policies with statements like:

> "*I haven't spoken to them about it and if they are stupid enough to fall for it they have to learn from it."*

Findings suggests that although the term phishing was not always known, owners-managers were able to articulate with clear examples (commonly Nigerian 419 email scams) of phishing related incidents that had occurred in their small businesses.

Researchers' interpretation regarding Phishing

Section 2.8 of the NISTIR 7621 is quite clear on how employees should be trained on security principles. It is simply not enough to tell employees "*if they are stupid enough to fall for it they have to learn from it."* The standard encourages owners-managers of small businesses to train "*employees who use any computer program containing sensitive information*", and that the employees should be taught how "*to properly use and protect that information*". Moreover, *Section 3.1* of NISTIR 7621 is very specific on security standards to be adhered to regarding emails requesting sensitive information. The standard suggests that *"beware of emails which ask for sensitive personal or financial information – regardless of who the email appears to be from. No responsible business will ask for sensitive information in an email".*

We noted that owners-managers did not have enough understanding to consider phishing as a big-enough risk that would require formal training. The suggestion that "*they had to learn from it*" neutralized this tenet. In terms of appropriating a measure for risk we interpreted and assigned this neutralization as H **= *high risk,*** this is shown by **Table 2** above. This means that the adopted neutralization may have a high impact to reputation and litigation.

Storage of Personal Data

From the interviews held, it emerged that there was a less rigid approach towards keeping personal data safe. Statements such as the one below from interviewee from organization 3 confirms this:

> *"There is no specific place, it's mostly company information and we store it everywhere."*

Although, restricting access to information seemed to have been fundamentally understood by the small business organizations, but beyond this, diminutive initiatives existed to follow accepted standards and guidelines. Phrases such as *"…everybody has access to the information…the business is so small"* tended to neutralize the possibility of securing personal information.

Researchers' interpretation regarding Storage of Personal Data

On the issue of personal data and privacy, *Section 2.10* of the NISTIR 7621 suggests that it is good practice to protect information from employees. The standard recommends that small businesses should "*not provide all data to any employee*" and that the employee should not have access "*to all systems,*

(for instance, financial, personnel, inventory, manufacturing, etc.)". The standard is clear: employees should only have information that is needed to do their jobs.

Minimal compliance with this provision was noted to be evident. From the owners-managers point of view, and how they rationalized this was that it would have been difficult to adhere to *Section 2.10* of the NISTIR. In terms of appropriating a measure for risk we interpreted and assigned this neutralization as H **= *high risk,*** this is shown by **Table 2**. This means the adopted neutralization will possibly have an impact on profits and reputation. Consequently, risk of litigation might also be possibly high.

Access control

It emerged from the interview sessions that the small businesses had a less rigid approach towards how anyone and everyone was accessing company records. An interviewee from organization 3 pointed out that:

> *"…everybody has access to the information…the business is so small so everybody that works here [and needs] the information every day [gets it]… "*

Researchers' interpretation regarding Access control

Section 2.6 of the NISTIR 7621 has provided a standard for how small businesses should control physical access to computers and network equipment. According to this section small businesses should not "*allow unauthorized persons to have physical access to or to use any of your business computers*". We specifically observed and interpreted this neutralization as one that presented a lack of awareness and poor framing of the importance of access control. We see this as a primary reason this provision was not followed. The need to implement requisite controls was therefore neutralized by the size of the organizations. In terms of appropriating a measure for risk we interpreted and assigned this neutralization as H **= *high risk,*** this is shown by **Table 2**.

Based on the discussions and interpretation in the previous sections, we were able to summarize the NISTR policies pertinent to securing ICT for small business organizations and present them in the format of **Table 3**. **Table 3** attempts to answer the last research question regarding how neutralization should be addressed in these contexts so the owners-managers are better placed to manage cyber-security threats more effectively.

Implications for theory

The theory of neutralization introduced by Sykes and Matza (1957) suggest that correct action can be 'neutralized' by 'turning off inner protests'. We have demonstrated that neutralization is not necessarily confined in disciplines such as criminology but can be especially extended into the discipline of information systems. In this work, the theory of neutralization provides an actual lens that presents owners-managers as having applied neutralization in contexts ~~to~~ of managing information and cyber-security threats. The contribution that this work brings is the application of the theory of neutralization into the discipline of information systems security. From the theory of neutralization's perspective, owners-managers should therefore be constantly aware of their need to abide by good practice because they have a fiduciary obligation to themselves and the businesses they run. Owners-managers should be aware of how unwittingly problematic neutralization can be.

Table 3: '*We want to Do it Our Way': Addressing neutralization*

Values for Information Security	Manifestation of Neutralization: "We want to Do it Our way" Approach	Summary of interpretation	Mitigating Neutralization (Risk identified in Table 2) Why "We want to do it our Way" is unwittingly problematic for a good manager
Back-up and Storage	*"My clerk dropped [the] back up [disk]! Now I cannot restore and the data is lost!"*	It remains easy for a manger to 'pass-the-buck' on employees particularly if they fail to correctly interpret their own fiduciary responsibilities to the business. ***Section 2.5, NISTR 7621***	A good manager should ensure that the small business has policies that not only address backing up data but also how to recover the same data when needed.
Password complexity	*"…We started with passwords…but I asked them to remove…"*	It is important to consider innovative ways to eliminate 'password fatigue'. ***Section 2.9, NISTR 7621***	A good manager should ensure that information systems are protected using strong passwords while equally ensuring audit and regulatory compliance.
Secure Online Banking	*"restricting access to the online banking"*	A full '*lock-down'* has never worked as a security measure and is often seen by employees as counterproductive. ***Section 3.4, NISTR 7621***	A good manager should spot where the small business is most vulnerable. Consideration should be given to value of online transactions and targeted awareness training.
Policy on Phishing	"*I haven't spoken to them about it and if they are stupid enough to fall for it they have to learn from it."*	Employees may be unwittingly manipulated to get them to perform action that could harm small businesses. ***Section 2.8, 3.1, NISTR 7621***	A good manager should ensure they are conversant and continuously updated with technical standards that address the threat of phishing.
Storage of Personal Data	*"…everybody has access to the information…the business is so small"*	Small businesses tend to collect personal data in less structured/ formalized ways. This creates avenues for privacy violations on personal data. ***Section 2.10, NISTR 7621***	A good manager should ensure compliance of privacy legislation which deal with issues regarding how to best treat personal data.
Access control	*"…if my employees are doing things on their computers, how would I know?*	It is important to consider risks that could come from your own staff because many security incidents come from disgruntled staff who could turn out to be 'insider threat agents'. ***Section 2.6, NISTR 7621***	A good manager should recognize different types of employees, the different types of potential incidents that these employees could create and how such incidents could evolve overtime.

Implications for Practice

We note that neutralization may not be an ideal approach towards managing cyber-security risk in small businesses operating in South Africa, specifically since many of the observed decision points suggested by this study sample of owners-managers tend to be rationalized imperfectly. On the basis of the four cases provided, such rationalization goes contrary to solid and good standards such as NISTIR 7621. Neutralization may therefore be potentially detrimental particularly when actions constrain the proper

adoptions of standards. We provide a framework notably in **Table 3** above that would signify the importance of managing detrimental neutralization and how decision points suggested could be improved upon.

Generalization of Research

A critique of the approach used in this work is that it remains difficult to generalize the above findings particularly since the four cases used might not necessarily be representative of many small businesses across South Africa. Indeed Denzin (1983) has rejected the notion of generalization as a goal in qualitative research and suggests that 'every instance of social interaction, if thickly described represents a slice from the life world'. Nevertheless it remains possible to generalize this work partly because of the replicability of the findings across several populations if the same methods are used. If the same methods can be applied elsewhere, *it remains possible to assert that neutralization can be manifest beyond these four cases*. This idea is akin to Yin's (2003:49-53) '*Literal replication'* from a case study research.

CONCLUSION

The work presents an insightful understanding on how neutralization as an outcome of existing values held by owners-managers of small business within Gauteng, South Africa could create unintended consequences of generating risk. We noted that neutralization served as antecedents to information security risks. It is from such observation and work carried out that we have provided a conceptual model that could guide owners-managers on how neutralization can be mitigated. The research work provides new insight into the cognitive effects of neutralization to small IT-dependent business organizations of Gauteng that would generate unintended consequences to the security of systems. While this work is specific to the small business organizations of South Africa, a global debate of various psycho-cognitive approaches to information security is to be encouraged. This work provided such a platform.

REFERENCES

Baard, V. C. and van den Berg, A. (2004). Interactive information consulting system for South African small businesses – Part 1. *South African Journal of Information Management*, 6(2): 1 - 27.

Barlow J. B., Warkentin M., Ormond D. and Dennis, A.R. (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation, Computers & Security 39, 145-159.

Barrett, F.J. and Walsham G. (2004) "Making Contribution from Interpretive Case Studies: Examining Process of Construction and Use" Judge Institute of Management, University of Cambridge

Beck, U. (1992). *Risk Society*. London: SAGE.

Beheshti, H. M. (2004). The impact of IT on SME's in the United States. *Information Management and Computer Security*, 12(4):318-327.

Boucher, D. and Flowerday, S. (2011). Privacy: In pursuit of information security awareness. Information Security South Africa (ISSA). In proceeding of: Information Security South Africa Conference 2011, Hyatt Regency Hotel, Rosebank, Johannesburg, South Africa, August 15-17, 2011. Proceedings ISSA 2011

Bougaardt, G. and Kyobe, M. (2011) Investigating the Factors Inhibiting SMEs from Recorgnizing and Measuring Losses From Cyber Crime in South Africa, *Proceedings of the 2nd International Conference on Information Management and Evaluation*, 27-28 April 2011, Ryerson University, Toronto Canada.

Bhattacharya, D. (2011). Leadership styles and information security in small business. *Information Management and Computer Security*, 19(5):300-312.

Blumberg, B., Cooper, D. R. and Schindler, P. S. (2008). *Business Research Methods (Second European Edition)*. McGraw-Hill Education.

Carkenord, B. (2009). *Seven Steps to Mastering Business Analysis.* J.Ross Publishers, 2009

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20:1 DOI: 10.1237/ISRE.1070.0160

Denzin, N. (1983). Interpretive interactionism. *Beyond method: Strategies for Social Research*. Morgan, G., Ed., Sage, Beverley Hills**:** 129-146.

Denzin, N.K. (1989) *Interpretive Interactionism*. London SAGE.

Furnell, S. M., Gennatou, M. and Dowland, P. S. (2002). A Prototype Tool for information security awareness and training. *Logistics Information Management*, 15(5):352-357.

Gauteng Provincial Government. (2010). *Gauteng SMME Policy Framework (2010-2014).* Gauteng: Department of Economic Development. Available from: http://www.ecodev.gpg.gov.za/policies/Documents/Gauteng%20SMME%20Policy%20Framework%20Revised%20100527.pdf

Grobler, M. and Jansen van Vuuren, J. (2010). *Broadband broadens scope for cyber crime in Africa.* Information Security for South Africa (ISSA): 1-8. Available from: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5588287&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5588287

Grobler, M., Jansen van Vuuren, J. and Zaaiman, J. (2011). Evaluating Cyber security Awareness in South Africa. 113-121. Available from: http://researchspace.csir.co.za/dspace/bitstream/10204/5108/1/Grobler1_2011.pdf?origin=publication_detail

Harper, D. (1998) "On the Authority of the Image: Visual Methods at the Crossroads", in N. Dezin and Y.S. Lincoln (eds) Collecting and Interpreting Qualitative Materials. London. SAGE pp. 717-732.

Heier, D.A. (2014) Utilizing NIST Guidelines for Small Business Security Assessment. *International Journal of Computer Science and Information Security* 1(2), 34-39.

Idrach, W.G., (2011) Do SMEs have the right attitude to security? *Computer Fraud & Security*, 18-20

Im, G., and Baskerville, R. (2005). A Longitudinal Study Of Information System Threat Categories: The Enduring Problem Of Human Error. *The Database for Advances in Information Systems*, 36 (4), pp. 68-79.

Johnson, P., Buehring, A., Cassell, C. and Symon, G. (2007). Defining qualitative management research: an empirical investigation. *Qualitative Research in Organizations and Management: An International Journal*, 2(1):23-42.

Kruger, H. A. and Kearney, W. D. (2008). Consensus ranking - An ICT security awareness case study. *Elsevier*, 27 (7-8): 254-259.

Kruger, H., Drevin, L. and Steyn, T. (2010). A vocabulary test to assess information security awareness. *Emerald*, 18(5):316-327.

Li, X. Zhu, Z. and Pan, X. (2012) Knowledge Cultivating for Intelligent Decision Making in Small and Middle Businesses, *Procedia Computer Science* 1: 2479–2488.

Mcnally J.S. (2013) The 2013 COSO Framework and SOX Compliance: One Approach to an Effective Transition. *Strategic Finance* 45-52.

Myers, M. (2013) *Qualitative Research in Business & Management*, 2nd Ed, Sage, Thousand Oaks, California.

Perks, S. (2010). Problem-solving techniques of growing very small businesses. *Journal of Enterprising Communities: People and Places in the Global Economy*, 4(3):220-233

Ponemon Institute.(2013) State of the endpoint 2012.

Salifu, A. (2008). The impact of internet crime on development. *Journal of Financial Crime*, 15(4):432-443.

Sangani, N.K. and Vijayakumar, B. (2012)"Cyber Security Scenarios and Control for Small and Medium Enterprises", *Informatica Economica* , 6 (2): 58-71.

Saunders, M., Lewis, P. and Thornhill, A. (2009). *Research methods for business students.* Prentice Hall.

SBP. (2009, August). *Small business development in South Africa*. SBP: business environment specialists. Available from: http://www.sbp.org.za/uploads/media/SBP_ALERT_smme_development_in_SA.pdf

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

SouthAfrica.info. (2012). *Gauteng province, South Africa*. Available from: http://www.southafrica.info/about/geography/gauteng.htm#.UqQZP_QW3Gw.

Stats SA. (2012). *Census 2011 Municipal report – Gauteng.* Statistics South Africa. Available from: http://www.statssa.gov.za/Census2011/Products/GP_Municipal_Report.pdf

Sykes G, Matza D. (1957) Techniques of neutralization: a theory of delinquency. American Sociological Review 22(6): 664-670.

Thomson, M. (2008). Making information security awareness and training more effective. *Information Security Journal: A Global Perspective*, 207-227. Available from: http://dl.acm.org/citation.cfm?id=1477818

Tsohou, A., Kokolakis, S. and Karyda, M. (2008). Process-variance models in information security awareness research. *Information Management and Computer Security*, 16(3):271-287.

Turner, D. W. (2010). Qualitative Interview Design: A Practical Guide for Novice Investigators. *The Qualitative Report*, 15(3):754-760.

Upfold, C.and Sewry, D. (2005). An investigation of information security in small and medium enterprises (SME's) in the Eastern Cape. Available from: http://eprints.ru.ac.za/2702/

Walsham, G. (1995) "Interpretive Case Studies in IS Research: Nature and Methods." European Journal of Information Systems Vol. 4:2 pp. 74-81

Warkentin, M. and Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2) 101-105.

Yildirim E.Y., Akalp G., Aytac, S. and Bayram, N. (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information* Management 31, 360–365

Yin, R. (2003). *Case Study Research Design and Methods*. Third Edition, Applied Social Research Methods Series, Sage Publications, Thousand Oaks, CA.