THE RISK OF USERS' NEGATIVE BEHAVIOURS INFLUENCE ON INFORMATION SECURITY COMPLIANCE POLICY IN ORGANIZATIONS

Godrey Cyprian Maphanga*, Osden Jokonya**

* Tshwane University of Technology, Department of Informatics, South Africa
** North-West University, Mafikeng Campus, South Africa

OPEN ACCESS

How to cite this paper:
Maphanga, G.C., & Jokonya, O. (2017). The risk of users' negative behaviours influence on information security compliance policy in organizations. *Risk Governance and Control: Financial Markets & Institutions, 7(4),* 30-40
http://doi.org/10.22495/rgc7i4art4

ISSN Online: 2077-4303
ISSN Print: 2077-429X

Received: 31.08.2016
Accepted: 22.11.2016

JEL Classification: D8, D81
DOI: 10.22495/rgc7i4art4

Abstract

The focus of information security has traditionally been on technological issues, and organizations have long been using technological controls to protect information assets. In spite of all these efforts there is still a significant level of non-compliance to information security compliance by employees in organizations. Information security also comes in non-technical forms that the technical controls cannot fully address without the cooperation of employees. This study investigates the factors influencing end-user resistance to information security compliance in organizations.
The study reviews the related literature to understand why and how end-user resistance develops. The paper adopted the qualitative research methodology which enabled the researcher to investigate end-users' attitudes towards information security compliance in the organization; using a single case study. The study results indicate that end-user resistance is mainly a result of lack of training and awareness of information security policies in the organization. The study contributed to our understanding of end-user resistance of information security in organizations. It also contributed to the emerging body of knowledge on behavioural issues of information security in organizations.

Keywords: Information, Information Security, End-User Resistance, Compliance, Case Study Research, Qualitative, Security Policy, Interpretive, Paradigm

1. INTRODUCTION

Information is one of the resources that organizations are heavily dependent on and many organizations today treat information and the associated information technology as vital organizational assets (Mellado, Sanchez, Medina & Piattini, 2013). These organizational information assets are vulnerable to many security breaches and threats that can inflict various types of damage and affect business continuity (Peltier, Peltier & Blackley, 2005). The destructions due to information security breaches and threat incidents warrants organizations to implement effective information security measures in order to protect the organizational information assets (Kim & Solomon, 2012).

1.1. Background of the study

Organizations have long been using technical controls to protect information assets (Bulgurcu, Cavusoglu & Benbasat, 2010). In spite of all these efforts there is still a significant level of non-compliance to information security in organizations and enforcement of security has always been a critical challenge due to the relatively discretionary nature of adherence (Rastogi & Von Solms, 2012). The technical controls guiding the protection of information assets are proving to solve only part of the problem as there is also a need to consider the human factor which is a critical issue in the information security chain (Bulgurcu et al., 2010).

Human factors have long been noted as an important area in the information security architecture (Shehri, 2012), because information security also comes in non-technical forms that technical controls cannot fully address without human cooperation (Fitzgerald, 2012). One of the critical success factors of information security compliance in the organization is the behaviour of users of information and related information technology commonly known as 'end-users' (Rastogi et al., 2012). The end-users can be both a threat and a resource in information security, and as a consequence information security management of employees is an important part of the total

information security management in organizations (Shehri, 2012). Although the end-users have adopted the various security technologies, there is still a high rate of non-compliance to information security in organizations caused by end-user resistance (Shehri, 2012).

Since the 20th century, organizations have faced end-user resistance, which has long been acknowledged as a critical issue during implementation. Although the literature recognizes the importance of end-user resistance, little attention has been paid to it in information security (Rivard & Lapointe, 2012). The objective of this study is therefore to investigate the factors influencing end-user resistance towards information security in organizations. The main research question is: What are the factors influencing end-user resistance towards information security compliance in organizations? The rest of the paper is structured as follows: Section 2 is the literature review, section 3 is the research methodology used for the study, section 4 is the results of the study and section 5 is the discussion and conclusion of the study.

2. LITERATURE REVIEW

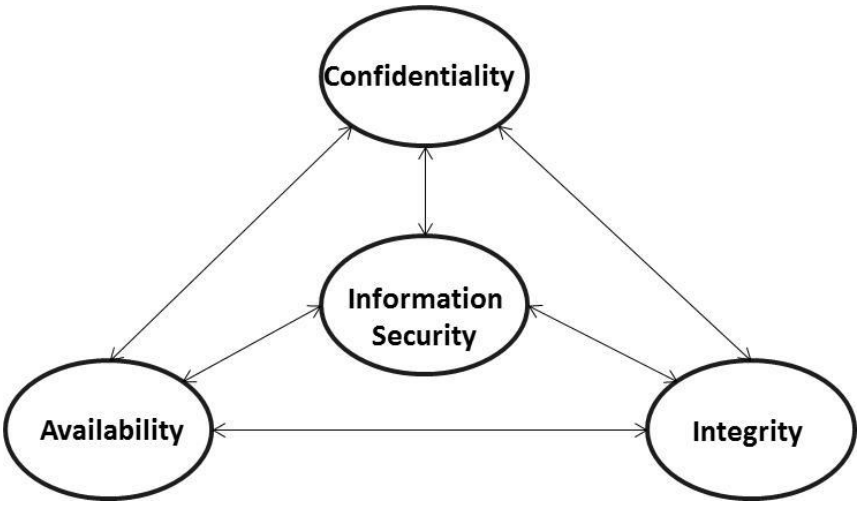
Throughout the years, organizations have experienced numerous system losses which have had a direct impact on their most valuable asset, which is information and therefore, as a result, information should be well protected and secured (Khan et al., 2011). Information is one of the resources that organizations are heavily dependent on (Kim et al., 2012) and has become one of the most important strategic organizational assets as it adds value to organizations (Mellado et al., 2013). Most organizations today treat information and the associated information technology as vital organizational assets. These information assets not only provide a competitive edge to the organizations; but in most cases are critical for the survival of the organizations (Rastogi et al., 2012). Organizational employees who have access to an organization's information and information systems, pose considerable intentional and accidental security risks to organizational information assets (Posey, Roberts, Lowry & Hightower, 2014).

Today's economy depends on the secure flow of information within and across organizations, thus making information security an issue of vital importance (Yanus & Shin, 2007). Therefore as a result of information intensive organizations, secured management of information has become an important issue (Herath & Rao, 2009). Most information security challenges in organizations today are addressed through the use of security tools and technologies. Although these tools and technologies are an integral part, it is argued that they alone are not sufficient to address information security problems (Posey et al., 2014). Developing an appropriate and affordable mechanism to protect an organization ICT infrastructure, systems and data is critical (Mackay et al., 2013).

The information security triad is a fundamental concept in information security and ensuring that the three facets of the triad are protected is an important step in designing any secure system (Merkow & Breithaupt (2006). The information security triad often referred to as CIA triad consist of:

1. **Confidentiality:** involves protecting the information from disclosure to unauthorized parties;
2. **Integrity:** involves protecting the information from being modified by unauthorized parties; and
3. **Availability:** involves ensuring that authorized parties are able to access the information when needed.

Figure 1. CIA Triad (Adapted from Merkow & Breithaupt,2006)



Information security should therefore ensure the protection of information, and the systems that store or process it; and this protection is against risks that would lead to unauthorized access, use, disclosure, disruption, modification or destruction of information (Johnson, 2011).

- **Information security breaches**

The growth in organizations using ICT coupled with information security breach incidents, have prompted organizations to implement effective

controls (Fitzgerald, 2012). Technical controls have traditionally received the most attention from information security professionals as the primary means of preventing information security breaches (Posey et al., 2014). These controls are largely intended to help organizations protect their information assets from any inadvertent or malicious harm or damage with the minimal level of user knowledge or input (Mackay et al., 2013). Although organizations spend more resources on technical controls to safeguard information security; empirical evidence has demonstrated that the number and severity of incidents are continuously increasing (Haeussinger & Kranz, 2013). The effective management of information security requires a combination of both technical and procedural controls to manage information security risks (Kearney & Kruger, 2006). The implementation of effective information security controls is thus dependent upon the creation of a security positive environment where everybody understands and complies (Bulgurcu et al., 2010).

- **Information security policies**

Information security policies involve the documentation of enterprise wide decisions on handling and protection of information (Peltier et al., 2005). Today corporate organizations develop information security policies to ensure that their infrastructure is secured from unauthorized access and protected from loss of sensitive data. A lack of these policies can lead to information security breaches (Herath & Rao, 2009). The focus of the organizational information security policy framework is to reduce the exposure to risks, threats and vulnerabilities (Kim & Solomon, 2012). Moving beyond the drafting and implementation of policies and standards; each business unit, through its management, has the responsibility to ensure enforcement and constant compliance with those policies and standards (Peltier et al., 2005). While the defined policies may be clear and detailed, the result may not turn out to be as desired, especially with regard to information security (Herath & Rao, 2009). The existence of formal information security policies does not necessarily mean that employees will adhere to the rules; subsequently employees need to be aware of the security practices prescribed in the firm's policy (Gundu & Flowerday, 2013).

- **Information security awareness**

The lack of information security awareness amongst end-users has long been recognized as a significant vulnerability in any ICT system and increasing the level of end-user awareness can be achieved by building an information security awareness culture (Mackay et al., 2013). Information security awareness is often an overlooked factor in an information security programme. Many organizations increase the use of advanced security technologies and continuously train their security professionals while very little is done to increase the information security awareness amongst the end-users, making them the weakest link in the organization (Aloul, 2012). Studies have shown that although information security awareness is proposed in every non-technical approach, it is still the least practised approach Mackay et al., 2013).

The information security behaviour of end-users can only be changed by raising the level of information security awareness whereby all employees are educated in the basics of information security to ensure that they understand and engage in the behaviours expected of them so that they can become vigilant (Kim et al., 2012). Previous studies argue that the security education, training and awareness programs influence information security behaviours positively and raise employees consciousness about the importance of information security (Haeussinger & Kranz, 2013). Gaining senior management buy-in is the first step and senior management must not only develop awareness also ensure an effective implementation strategy (Johnson, 2011). Nothing yields as much return on investment (ROI) as information security awareness (Kim et al., 2012) and education will influence and extend end-users' knowledge on information security, irrespective of their fields of study (Shehri, 2012).

- **Information security personnel**

The role of information security personnel has changed over years and it will always be an organization-wide responsibility that touches every person (Peltier et al., 2005). The senior management together with IT management, including security professionals of an organization, are primarily responsible for implementing, ensuring and managing information security that protects the organization's information assets (Herath & Rao, 2009). Senior management involvement is important for successful implementation of an information security program in organizations (Peltier et al., 2005). However uniform participation in the information security is necessary; from senior management, through business unit management, to every individual member of an organization, in an effort to support the organization in achieving its information security aims and objectives (Peltier et al., 2005).

- **Information security end-users**

The literature recognizes that end-users may pose information security challenge to an organization because of their ignorance, mistakes and deliberate acts (Bulgurcu et al., 2010). Regardless of the technological security measures in place, the success of an organization's security efforts relies on the end-users cooperation (Posey et al., 2014). Human factors has long been noted as an important area of the information security architecture (Shehri, 2012), End-users often lack awareness about the best information security practice result in high rate of non-compliance in organizations (Shehri, 2012). Every day new incidents of information security breaches, threats, risks are reported which are caused by human errors and lack of information security awareness. Many researchers claim that the human component of any information security framework is the weakest link (Kim et al., 2012; Shehri, 2012).

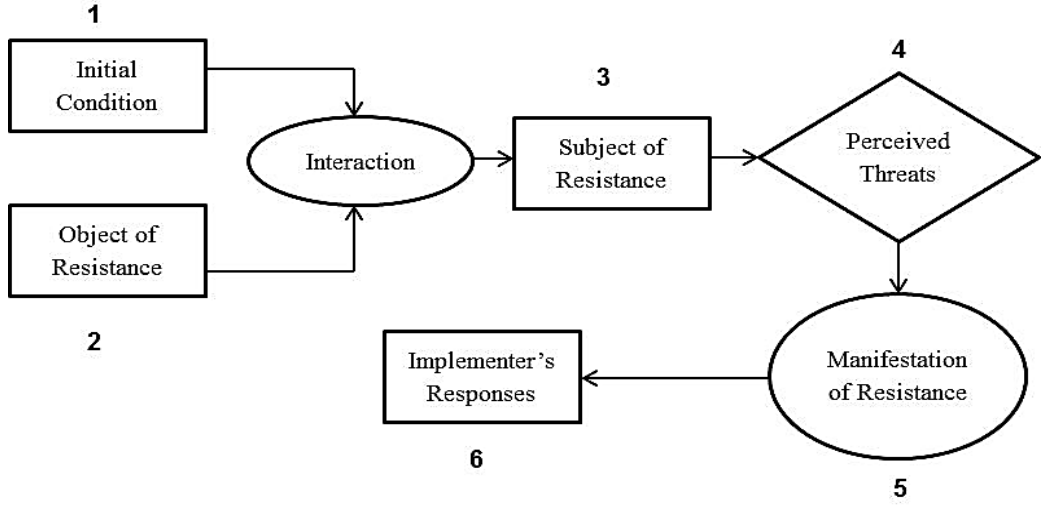
Previous studies on information technology implementation recognized resistance as a critical variable (Rivard & Lapointe, 2005). While some saw resistance as a barrier to be removed, others saw it as a means by which end-users communicate their discomfort with a system that might be flawed. While previous researchers have explored the reasons for end-user resistance, there are gaps in understanding how end-users evaluate change related to new information systems and desire to resist it (Kim et al., 2012). Information systems implementation projects have historically been plagued by failures in which end-user resistance has consistently been identified as a salient reason (Posey et al., 2014).

While losses and threats have been noted as causes of end-user resistance in previous studies, there are gaps in understanding of the psychological and decision making mechanisms underlying resistance (Kim et al., 2012). Notwithstanding the nature of end-users resistance to information security compliance, organizations have to address it. Although the literature recognizes the importance of user resistance, it has paid little attention to organization's responses and their effect when resistance occurs (Rivard & Lapointe, 2012). The next section discusses the theoretical framework that guides the study.

2.1. Theoretical framework

The study adopted Rivard & Lapointe's (2012) multi-level conceptual framework to help understand end-users' resistance toward information security in organizations. The Rivard & Lapointe (2012) multi-level conceptual framework has six basic elements (Figure 2). These six basic elements of end-user manifestation of resistance are: initial conditions, object of resistance, subject of resistance, perceived threats, manifestation of resistance and implementers' responses respectively (Figure 2).

Figure 2. Theoretical Framework (Source: Rivard & Lapointe, 2005)



- **Initial condition**

The initial condition presents the characteristics of the environment that interacts with the object of resistance, which influences the assessment that users make of the situation regarding outcomes in terms of future performance (Rivard & Lapointe, 2012). It is essential to keep the employees constantly aware of information security threats and educate them towards using good security (Shehri, 2012).

- **Object of resistance**

The object of resistance represents the target of resistance behaviours, which in some cases is the system itself and its features, whereas in other cases it is associated with the significance that the system has to the end-users, such as loss of power (Rivard & Lapointe, 2012). Although organizations have adopted various technologies, end-users often lack awareness of security practice (Shehri, 2012).

- **Subject of resistance**

The subject of resistance represents the actor or actors exhibiting resistance behaviours which in some instances is an individual often referred to as an "end-user", but may also be a group of people or the organization itself (Rivard & Lapointe, 2012). The end-users are likely to exhibit two kinds of resistance behaviours which are intentional or unintentional. The intentional behaviours occur when disgruntled end-users perform intentional disruptive behaviours and, unintentional behaviours occurs when uninformed end-users make naïve mistakes (Gundu & Flowerday, 2013).

- **Perceived threats**

The perceived threats represents the negative assessments that end-users make of the ICT implementation whereby resistance stems from negative end-user assessments between their inputs and the outcomes of their interaction with ICT (Rivard & Lapointe, 2012). The attitude of end-users towards information security compliance is important because, unless they believe that information security is important, they are unlikely to adhere to security policies irrespective of how much they know about security requirements (Gundu & Flowerday, 2013).

- **Manifestation of resistance**

The manifestation of resistance represents the set of behaviours enacted by end-users to manifest some discontent with the implementation of ICT systems (Rivard & Lapointe, 2012). Manifestation can be evident when end-users continue to exhibit significant levels of non-compliance towards information security policies and controls in an organization (Rastogi et al., 2012).

- **Implementers' responses**

The implementers' responses represent those responsible for the introduction of the technology, as well as those responsible for the successful use of the implemented systems; as the key interventions made by these implementers may influence how resistance evolves (Rivard & Lapointe, 2012). Identifying the causes of end-user resistance and determining what can be done about them is considered one of the first responses that the implementers, should have when end-user resistance occurs (Rivard & Lapointe, 2012).

3. RESEARCH METHODOLOGY

The two most common research paradigms are the positivist paradigm, which is a scientific method based on rationalistic, empiricist philosophy, and the interpretive paradigm, which relies upon the participants' views of the situation being studied and recognising the impact on the research based on their own background and experiences (Knipe & Mackenzie, 2006). The study adopts the interpretive paradigm which enabled the researcher to look at the end-user attitudes towards information security compliance in the organization. Interpretive research helps to understand the world of human experience which is socially constructed relying on participants' views of the situation being studied (Knipe & Mackenzie, 2006). End-user resistance to information security compliance is real and everyone sees it from a different perspective, so it is impossible to establish universal truth, hence the interpretative research is more appropriate for this study.

3.1. Case study research strategy

The case study research was based on a medium size organization based in Pretoria, South Africa. The selected organization was found suitable for the study of end-users' resistance towards information security compliance as they were currently implementing new technologies in the organization. For confidentiality purposes the name of the organization will remain anonymous. The study looked at the end-user resistance towards information security in the organization. The case study research is recommended for studying information systems in organizations (Jokonya, 2016).

3.2. Research method

Research methods are mainly categorized either into quantitative or qualitative methods and the research method depends upon the phenomena under study. Clark & Creswell, (2010) differentiate two methods as follows: the quantitative method "as a type of research in which the researcher studies a problem that calls for an explanation" and qualitative method "as a type of research in which the researcher studies a problem that calls for exploration". It is therefore crucial to select the appropriate and relevant research method that will assist in addressing the research problem. This study adopted the qualitative research method which enabled the researcher to look at end-user attitudes towards information security in organizations. Since the end-users' subjective feelings and emotions are difficult or impossible to quantify the qualitative method was found appropriate for the study (Jokonya, 2016).

The qualitative research is best suited for research problems where the researcher needs to explore and learn from participants because important variables are unknown, and furthermore if the topic under study has been little studied and a need exists for further exploration (Clark et al., 2010). Information security involves people and as soon as people are involved, it is easier to assess their knowledge, attitude, reasoning, behaviours and opinions since the qualitative method is dependent on descriptions. It is especially suitable for behavioural sciences where the aim is to discover the underlying motives of human behaviour.

The qualitative research is interested in conducting in-depth studies of smaller populations and groups, as it does not seek to obtain data that can be applied across the population, instead researchers try to find out as much as possible about a smaller sample (Zemliansky, 2008). The qualitative method does not apply statistical methods of quantification to the results. Therefore the study will focus on a smaller group to understand their attitudes towards information security.

3.3. Sampling technique

The study made use of a purposive sampling technique in order to carefully select the participants based on their relevance and level of knowledge on the underpinned study (Clark et al, 2010). The purposive sampling was intentionally used to select individuals to learn about end-user resistance towards information security. This sampling technique is appropriate for qualitative research to identify the best participants to learn about the central phenomenon (Clark et al., 2010). The purposive sampling was successfully implemented because it gave the researcher an opportunity to sample relevant knowledgeable respondents on the phenomena under study, based on their day to day responsibilities within the organization. These responses provide the most valid or credible results because they reflect the characteristics of the population from which they were selected.

The study targeted 20 participants from the organization with knowledge of the phenomena, under study. The targeted participants were the end-users (10), ICT personnel (5) and senior management (5). The main goal was to focus on particular characteristics of the population that were of interest which would best enable the research to

answer the research question. The study made use of a case study protocol, described as a set of guidelines that can be used to structure and govern a research project.

3.4. Data collection

Data was collected from the employees of the organization through both open-ended and close-ended questionnaires. Questionnaires are the most convenient, economical way of gathering information from people and they could be used to gather either quantitative or qualitative data. The questionnaire was designed in such a way that respondents had freedom to express their views in response to the question asked without any influence or clues from the researcher. The targeted respondents for close-ended questionnaires were the end-users, and open ended questionnaires were for both the ICT personnel and senior management from the organization. The questionnaires were delivered personally to the targeted respondents and the researcher encouraged them by explaining the purpose of the study and how the results could benefit them. The study employed different techniques to address ethical issues such as anonymity of respondents and informed consent of participants.

3.5. Data analysis

In terms of data analysis the study made use of the content analysis approach, which is applicable for this kind of questionnaire, to effect qualitative data reduction and apply a sense-making effort that takes a volume of qualitative material and attempts to identify core concepts and meanings. All the questionnaires were coded based on the total number of respondents in order to prevent misrepresentation of respondent's data and the data was analysed through a histogram. Histograms provide presentations of observations of a given code summarizing findings of each respondent with and with the area of the bar representing the value of the frequency within an interval.

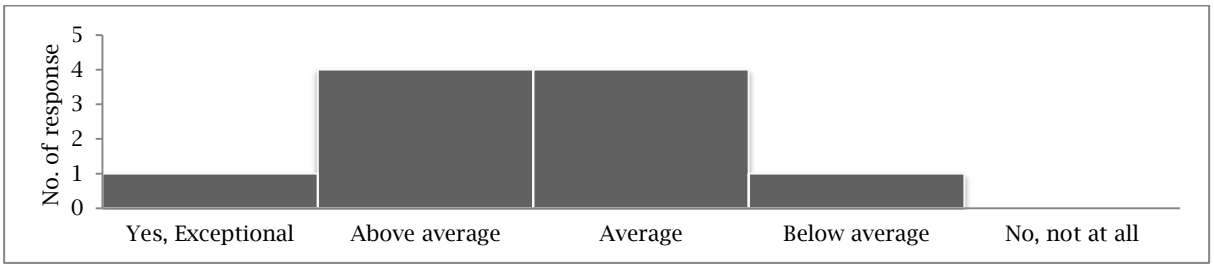
4. RESEARCH RESULTS

This section presents the results from the analysed data. The research study sought to investigate the factors influencing end-user resistance to information security compliance through the employees of the identified organization, with particular focus on three groups who were the end-users, ICT personnel and senior management. In addition the study investigated the six elements of end-user resistance in order to understand the factors influencing end-user resistance. The six elements of why and how end-user resistance develops are: (1) initial condition (2) subject of resistance (3) manifestation of resistance (4) object of resistance (5) perceived threats and (6) implementers responses respectively. The collected qualitative data was summarized, presented in the form of histograms and further translated into narrative discussions, whereby the researcher shortened the details of the findings in a narrative form.

4.1. Basic knowledge of information security in the organization

The end-users were evaluated on their basic understanding of information security in order to identify if they had a broader understanding of the phenomena under study. Most of the respondents demonstrated a general understanding of information security in the organization. However, some of the respondents' understanding was at an average level, with few at an exceptional level and below average respectively. The results suggest that there are gaps between the end-users in terms of their information security knowledge.

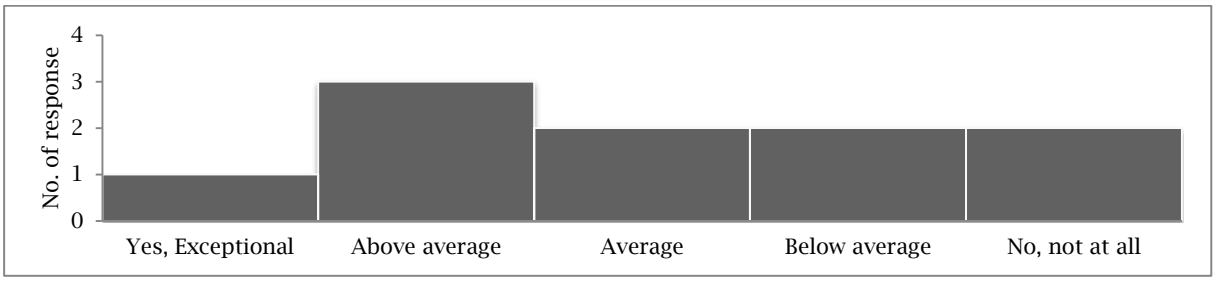
Figure 3. Knowledge of information security in the organization



4.1.2. Basic knowledge of documented information security policy in the organization

The end-users were evaluated on their knowledge of the existence of security policy within the organization. Most of the respondents demonstrated a minimal knowledge of the information security policy in place within the organization. The results suggest that the majority of the end-users were not aware of the existence of an information security policy in the organization.

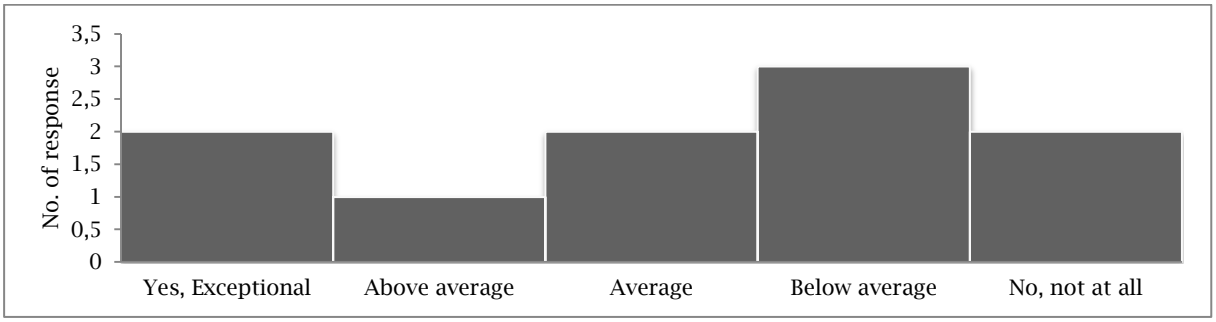
Figure 4. Basic knowledge of documented information security policy in the organization



4.1.3. Basic awareness of information security threats and breaches in the organization

The end-users were evaluated to establish if they were abreast of issues about information security threats and breaches. Most respondents are aware of information security breaches and threats issues. The results suggest that there is awareness and communication on information security threats and breaches in the organization.

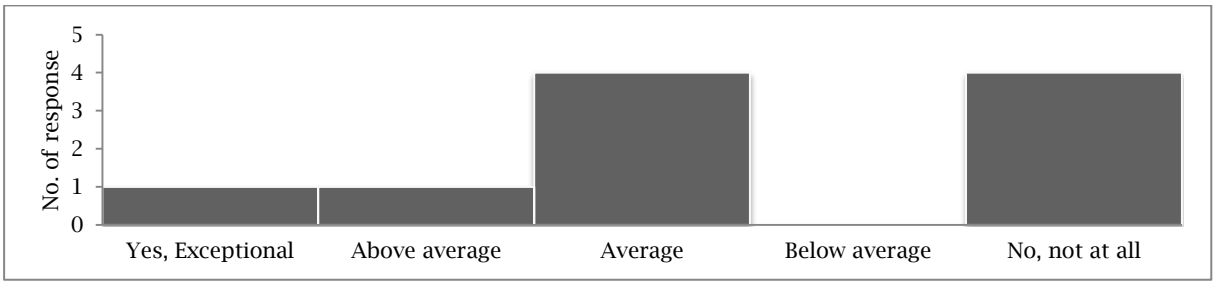
Figure 5. Awareness of information security threats and breaches in the organization



4.1.4. Basic training on information security issues in the organization

The end-users were asked if they had received training on information security in the organization. The results showed that some end-users had never received training, with a few having received training. The results indicate that end-users are not receiving training on information security issues in the organization.

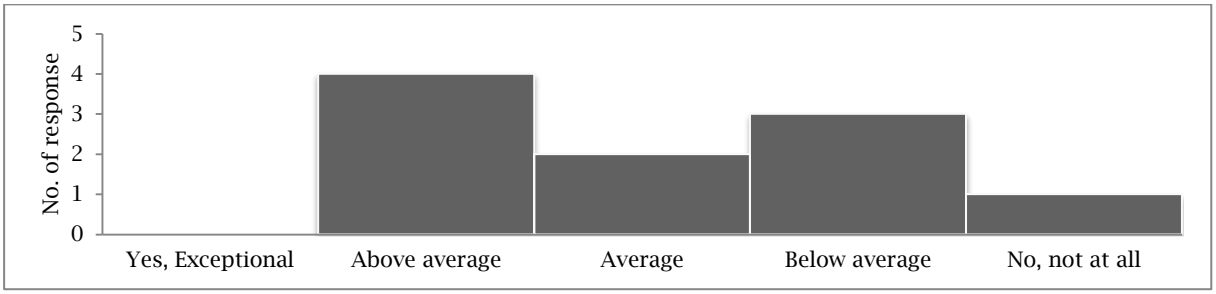
Figure 6. Training on information security issues in the organization



4.1.5. Communication of information security issues in the organization

The communication of information security issues by the organization was evaluated among the end-users. The results indicate that the organization was mostly at an average level when it comes to communication of information security issues. Some end-users indicated that the organization was not communicating at all. These results showed that there are inconsistencies with regard to the communication of information security issues.

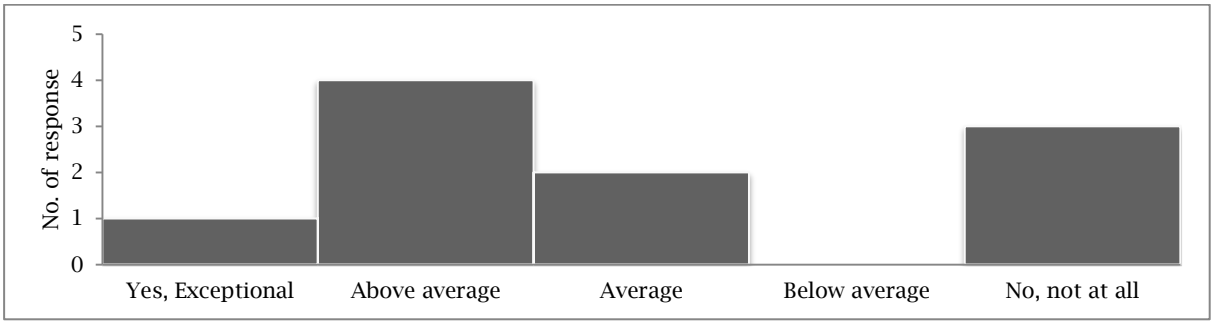
Figure 7. Communication of information security issues in the organization



4.1.6. Possession of information security skills

The end-users were evaluated on the basic necessary skills that they possess that can assist in ensuring information security in the organization. The results showed that most of the end-users did not have the basic necessary skills needed to ensure effective and efficient information security in the organization. The results indicate that the adequate skills necessary for ensuring effective and efficient information security amongst the end-users in the organization were at different levels.

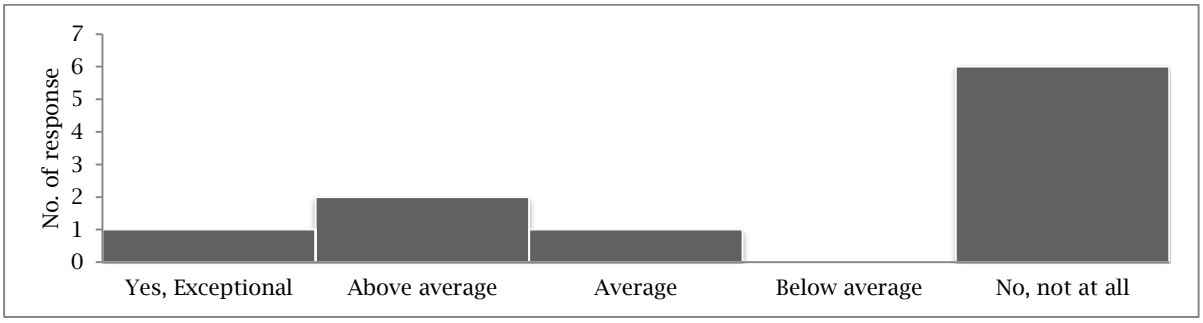
Figure 8. Possession of information security skills



4.1.7. Attendance of information security awareness sessions in the organization

The end-users were evaluated on whether they attended any information security awareness sessions in the organization. The results indicate that most end-users never attended any formal information security awareness sessions within the organization. Based on these outcomes there is still a need to understand whether the organization had ever implemented any information security awareness sessions in an effort to promote a positive information security culture within the organization and this was assessed in the next sub-questions with the ICT personnel and senior management.

Figure 9. Attendance of information security awareness in the organization



4.2. The ICT Professionals

The reviewed literature demonstrated that end-user resistance is a critical issue and as a result the implementers who are mainly the business managers, functional managers and ICT professionals have to address it. In an effort to address the research question, the next section presents the exploration of factors influencing end-user resistance in information security, through the data collected from the ICT professionals.

4.2.1. Existence of information security policy in the organization

The ICT personnel were evaluated on the existence of information security policy providing guidance on how information should be managed in the organization. The results from the respondents demonstrated that the organization does not have a formal information security policy. One of the respondents, when responding to the kind of policy existing in the organization, indicated that the organization has; "*Code of ethics on internet usage and IT*"; another respondent indicated that "*policies are our induction manual under IT*"; and the other respondent indicated that the only policy in place is the *"USB policy-no USB stick should be used into the computer before it has been screened / scanned by the personnel".* Based on these results, it is evident that the organization did not have any formal information security policy in place.

4.2.2. Compliance of the end-users to the information security policy in the organization

The ICT personnel were evaluated on the compliance of end-users with the information security policy in the organization. One of the respondents, indicated that *"they do; some do take chances, but mostly end-users comply with the set and approved policies and procedures"*; another respondent indicated that *"yes; 95% of the end-users register the laptops, overhead projectors before they leave for training";* and other respondents indicated only "*yes".* Based on these results in comparison to the first question, it is not clear as to what are the end-users complying with, as there seem to be many rules that are not formally documented as part of the information security policy in the organization.

4.2.3. End-users practising the appropriate set standards of information security in organizations

The ICT personnel were evaluated in order to understand whether the end-users are practising the appropriate set standards of information security within the organization. One of the respondents indicated that *"no, we do have isolated incidences of high data usage as a result of unauthorized downloads and policy violations";* another respondent indicated that *"no, not all but 90% of end-users are practicing the set standards;* and other respondent indicated that *"yes, some hate it, but implement it".* Based on these results it is evident that the organization was facing non-compliance issues from end-users from time to time.

4.2.4. End-users training on information security policy and security standards in the organization

The ICT personnel were evaluated in order to assess whether all the end-users were trained on the information security policy and security standards in the organization. One of the respondent stated that *"yes, we have induction on various fields and divisions in the office"*; another responded asserted that *"training is compulsory and happens on induction. Its mandatory to receive training";* and another indicated that *"yes we have induction in the organization and training for both new and old end-users".* The results demonstrate that the end-users were inducted in the organization as part of the company policy.

4.2.5. The perceptions of end-users towards information security in the organization

The ICT personnel were evaluated in order to assess the statements often made by the end-users towards information security in the organization. One of the respondents stated that *"some hate the security systems in place as they can't log on to social media all day and download stuff";* another respondent further stated that" *most hate policies but these policies are in place to protect the organization - some see it as IT Department is controlling";* whereas another respondent indicated that *"ignorance, people tend to forget on what they should apply".* The results demonstrate that the end-users are not in favour of the current information security systems in place.

4.2.6. The methods used to communicate information security issues to end-users in the organization

The ICT personnel were evaluated in order to identify the methods currently utilized by the organization to communicate information security issues to the end-users. One of the respondents indicated that information security issues are communicated to end-users *"via bulk sms",* another respondent stated that "*they get called to 1 on 1 meetings to discuss information security breaches, in other cases bulk e-mails are sent out to alert all users on scams / phishers*"; whereas one respondent stated that *"no formal methods exist".* The results demonstrate that the organization did not have any formal methods of communicating information security issues to the end-users in the organization.

4.3. The senior management results

The senior management were also evaluated using the same criteria as the ICT personnel; however their responses were separated based on the fact that senior managers are more into strategic issues and hence it is crucial to understand their perceptions in terms of the phenomena under study as the vision bearers of the organization.

4.3.1. Existence of information security policy in the organization

Management were evaluated to test the existence of an information security policy in the organization. One of the respondents when responding to the kind of information security policy in existence in the organization indicated that the organization has; "*information management policy; not sure if it is officially documented";* and all the other respondents indicated that *"all information security is managed and controlled by the ICT manager".* The responses from the senior management indicate that the majority of the respondents were of the opinion that the ICT manager was responsible for management of the information security policy in the organization.

4.3.2. Compliance of the end-users to the information security policy in the organization

Management were evaluated in an effort to obtain an insight as to whether the end-users were complying with the approved information security policy. However, this question was already partially answered based on the responses from the ICT personnel, but it was still critical to get the senior management responses rather than to make an assumption. One of the respondents, when responding to the compliance of end-users to the approved information security policy in the organization; indicated that "*systems forces them to comply"*; other respondents indicated only *"yes"*; and another respondent indicated *"no not at all"*. The results demonstrate some inconsistencies from management on compliance to information security policy in the organization.

4.3.3. End-users' training on information security policy and other security standards in the organization

Management were evaluated in order to assess whether all the end-users were trained on the information security policy and other security standards in the organization. One of the respondents stated that "*only informal demonstration by the ICT Manager"*; another responded indicated that *"no; not all";* and the other respondents indicated *"yes", its mandatory to receive training";* and another indicated that *"yes we have induction in the organization and training for both new and old end-users".* The final results demonstrate that the end-users were informally trained and it could be further suggested that the training was on a one on one basis, hence there were inconsistencies in the responses.

4.3.4. The perceptions of end-users towards information security in the organization

Management were evaluated in order to assess the perceptions often held by the end-users towards information security in the organization. One of the respondents indicated that *"they are really not interested",* another respondent indicated that *"all agree that we must protect our information",* whereas another respondent indicated that *"they do not regard it as critical".* The results demonstrate that the end-users were really not keen towards information security in the organization. However there was another group that seemed to be keen and this indicates that there was an inconsistency amongst the end-users.

4.3.5. The methods used to communicate information security issues to end-users in the organization

Management were evaluated in order to identify the methods currently utilized by the organization to communicate information security issues to the end-users. The majority of the respondents indicated that information security issues were communicated to end-users through the *"ICT manager, via e-mail or verbal announcement at a meeting",* and other respondents indicated that "*at workshops and staff meetings*". On this basis it can be concluded that the organization did not have any formal methods of communicating information security issues to the end-users. The next section presents the discussion and conclusion of the study.

5. DISCUSSION

The objective of the study was to investigate the factors influencing end-user resistance towards information security in organizations. The results suggest that end-users do not really consider information security as an issue of vital importance. Most of the respondents showed little knowledge of an information security policy in the organization. The literature suggests that knowledge of information security policies is important to protect organizational integrity (Johnson, 2011). In addition, most of the respondents were not aware of the information security breaches and threats issues that affect organization. Information security breaches and threats can inflict various types of damages and affect business continuity (Peltier et al., 2005).

The results also show that some end-users had not received training on information security in the organization. Training is important to influence and extend end-users' knowledge in understanding information security (Shehri, 2012). In addition, the results showed a lack of communication on information security issues in the organization. Previous studies suggest that communication is important to provide end-users with information security knowledge (Khan et al., 2011). The results indicate end-users' lack of skills necessary for ensuring compliance in information security in the organization. The unskilled users put the organization systems at risk as they are an easy target by hackers (Aloul, 2012). The results also suggest a lack of formal information security awareness in the organization. Information security awareness helps improve end-users' knowledge and awareness of potential information security risks in the organization (Haeussinger & Kranz, 2013).

The management and ICT personnel responses support that the organization did not have a formal information security policy. An information security policy is important in providing guidelines to end-users on best practices (Bulgurcu et al., 2010).The study results suggest that most end-users did not comply with security standards since the organization did not have documented policies in place. This supports the literature that end-users are the weakest link in the information security chain in the organization (Yanus et al., 2007).

The results demonstrate that there were inconsistencies in the responses of end-users. The results indicate that the end-users' lack of interest towards information security in the organization, may be caused by lack of awareness, training and communication. The literature argues that unless they believe that information security is important, they are unlikely to comply with security requirements (Gundu & Flowerday, 2013). The results demonstrate that the organization did not have any formal methods of communicating information security issues to the end-users. Rastogi

et al., (2012) concur that communication is a key in information security because it informs the end-users about information security policies, controls and guidelines.

6. CONCLUSION

The study results suggest that information security in organizations consists of both technical and human elements that make it complex. If there is lack of attention in these elements the organization is bound to face information security risks. The study indicated that end-users often face difficulty when undertaking information security in the organization due to factors related to knowledge, awareness, training and skills. In the absence of support, it is therefore expected that end-users will avoid or bypass information security controls in organizations. Lack of information and awareness have seen most end-users perceive information security practices as time-consuming and obstacles to their work. Training, communication and awareness are important in reducing end-user resistance and creating a positive attitude towards information security compliance in organizations.

The study therefore suggests that organizations need to create an information security culture to reduce end-user resistance. The study therefore contributes to our understanding of factors influencing end-user resistance towards information security compliance in organizations which has been inadequately addressed in the literature. In addition the study also contributed to the emerging body of knowledge on behavioural issues of information security in organizations. The limitation of the study, conducted using a case study research strategy, is that the results cannot be generalised. However, the limitation may be taken as an opportunity of further studies on how end-user resistance toward information security in organizations can be reduced.

REFERENCES

1. Aloul, F. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology,* 3. https://doi.org/10.4304/jait.3.3.176-183
2. Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 34
3. Clark, V., & Creswell, J. (2010). *Understanding research.* New Jersey: Pearson
4. Fitzgerald, T. (2012). *Information security governance simplified.* Parkway: CRC Press.
5. Gundu, T., & Flowerday, S.V. (2013). Ignorance to awareness: towards an information security process. *South African Institute of Electrical Engineers,* 104.
6. Haeussinger, F., & Kranz, J. (2013). Information security awareness: its antecedents and mediating effects on security compliant behaviour. Paper presented at the *Thirty Fourth International Conference on Information Systems.*
7. Herath, T., & Rao, H. (2009). Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. 47(2), 154-165.
8. Johnson, R. (2011). *Security policies and implementation issues.* Jones & Bartlett Learning.
9. Jokonya, O. (2016). Building and Validating Information Systems Theory using a Case Study Sequential Explanatory Mixed Methods Research, *20th Pacific Asia Conference on Information Systems (PACIS 2016) 27 June – 1 July Chiayi, Taiwan.*
10. Kearney, W., & Kruger, H. (2006). A prototype for assessing information security awareness. 25(4), Oxford: Elsevier Advanced Technology Publications
11. Khan, B., Algathbar, K., Nabi, S., & Khan, M. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management,* 5(26).
12. Kim, D., & Solomon, M. (2012). *Fundamentals of information systems security.* Jones & Bartlett Learning.
13. Knipe, S., & Mackenzie, N. (2006). Research dilemmas: paradigms, methods and methodology. *Issues in Educational Research,* 16.
14. Mackay, M., Balikhina, T., & Maqousi, A. (2013). An effective method for information security awareness raising initiatives. *International Journal of Computer Science and Information Technology,* 5(2).
15. Mellado, D. Sanchez, L., Medina, E., & Piattini, M. (2013). *IT security governance innovations.* Hershey: IGI Global. https://doi.org/10.4018/978-1-4666-2083-4
16. Merkow, M., & Breithaupt J. (2006) *Information Security Principles and Practices.* Pearson Prentice Hall, CA USA
17. Peltier, T., Peltier, J., & Blackley, J. (2005). *Information security fundamentals.* London: Auerbach Publications
18. Posey, C., Roberts, T., Lowry, P., & Hightower, R. (2014). Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management,* 51(5), 551-567. HTTPS://DOI.ORG/10.1016/J.IM.2014.03.009
19. Rastogi, R., & Von Solms, R. (2012). Information security service management. *Journal of Contemporary Management,* 9.
20. Rivard, S., & Lapointe, L. (2005). A multilevel model of resistance to information technology implementation. *MIS Quarterly,* 29(3), 462-491.
21. Rivard, S., & Lapointe, L. (2012). Information Technology Implementers Responses to User Resistance: Nature and Effects. *MIS Quarterly, 36(3).*
22. Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences,* 6(1).
23. Yanus, R., & Shin, N. (2007). *Critical success factors for managing and information security awareness program.* City: Pace University.
24. Zemliansky, P. (2008). Methods of discovery: *A guide to research writing* [Online]. Retrieved from the World Wide Web: Methods of discovery.net/ ?q=node/19.