Assessment on the level of information security awareness at the Government Pensions Administration Agency (GPAA)

Boitumelo Blessing Ikaneng

1540514

A consultancy report submitted to the Faculty of Commerce, Law, and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Business Administration

Johannesburg, 2018

Protocol number: WBS/BA 1540514/928

April 2018

DECLARATION

I, Boitumelo Blessing Ikaneng, declare that this consultancy report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Boitumelo Blessing Ikaneng

Signed at ……

On the …….. Day of …… 20…..

DEDICATION

I dedicate this study to my late mother, Nonceba Gwabeni and my late grandmother, Nozimbo Gwabeni.

ACKNOWLEDGEMENTS

Firstly, all praise and honour to the Lord for granting me the strength, serenity, commitment and determination to accomplish my dream.

To my sister, Keolebogile and my two kids Aobakwe and Mokgabo, your patience, emotional support and encouragement have resulted in this accomplishment.

My deepest appreciation goes to my Research Supervisor, Tetyana Loskutova. This study would not have been possible without her valuable guidance.

Special thanks to Eric Morudu, and Silindile Mkhize who have worked tirelessly to assist me with various aspects of my study including recommending appropriate statistical procedures, interpreting the resultant outputs, editing, proofreading and organising my overall research structure.

Lastly, to the Government Pension Administration Agency (GPAA) thank you for providing me with the platform to conduct my research. I am equally thankful to all who participated in this study.

SUPPLEMENTARY INFORMATION

Supervisor:	Tetyana Loskutova
Word count †:	18681
Supplementary files:	Appendix A – Information security survey
	Appendix B – Approval to conduct research
	Appendix C to E - Statistical analysis

† Including Executive Summary, References, etc.

Table of Contents

LIST OF TABLE

LIST OF FIGURES

EXECUTIVE SUMMARY

Literature confirms the significance of information security, and its importance due to increased reliance on information communication technology (ICT). This stems from the risks and threats associated with the high connectivity and interconnectedness of the current world. Information security awareness (ISA) in relation to employees has become topical, as there is a need for organisations to maintain a competitive advantage, legal compliance and an overall commercial image, which positively influences the organisation's cash flow and profitability.

Albeit, technology advances within the information security field, such as hardware, software, and networking system initiatives have been a pioneering shift towards the protection of information and even prevented threats of information security breaches. It does, however, remain that initiatives aimed at ISA are critical to all information security programmes. The successful application of initiatives and programmes aimed at ISA are dependent on the establishment of an appropriate initiative or programme, therefore the organisation’s level of ISA must first be established before a suitable information security awareness programme can be formulated and implemented.

This study used the survey research model to determine the level of employee awareness of information security within the Government Pensions Administration Agency (GPAA).The survey contained a range of questions and was used to gather data from employees of the Government Pensions Administration Agency. Statistical methods such as mean and standard deviation were utilised to analyse the data collected from respondents.

An analysis of the data suggests that there is generally a high level of information security awareness at the GPAA.

Keywords: Information security awareness; Information communication technology

1. INTRODUCTION

Chapter 10 of the Constitution of the Republic of South Africa regulates public administration in the Republic. Section 195 of the Constitution provides that public administration must adhere to the values and principles preserved in the constitution, which include: "The promotion of effective, efficient and economical use of resources; the provision of timely; accurate and information; which requires the public administration to be accountable to the public"(Africa, 1996).

Managing risks associated with security threats is becoming more and more important to both public and private organisations since violation of information security often has serious financial and reputational consequences. The state has valuable information that needs to be entrusted to people in order to get work done, therefore the security and management of state information is important for government departments. Ngoepe (2008) argued that better service delivery always begins with better information management practice. The challenge for many institutions today, is not only in investing and improving security software and services, but also about creating and improving security awareness of employees.

In order to address this challenge and manage the risk of security breaches, technical security measures and information security policies should be implemented. One way to manage and control security risks caused by human's lack of knowledge and wrong behaviour is in implementing information security awareness programs.

The regulation of information security management systems (ISMS) is prescribed by certain standards and frameworks i.e. ISO 27001, as they provide guidance and direction on establishing, implementing and monitoring ISMS. The standard also place emphasis on user awareness, making it evident that all users of system based information should be aware of information security policies and their contents, the security risks related and associated with utilising a specific organisation's various information systems, including implications on non-conformities.

The GPAA has a mandate to provide services to its clients within a specific turnaround time. The GPAA administers pension benefits for most of the employees of the government in South Africa. Government employees access these benefits

when they resign, retire or in the event of the members' death, where their dependents receive the benefits. The information and records of these members are managed and stored both electronically and manually. This makes the GPAA more susceptible to exposure, due to unauthorised access or intrusion, as information is likely not to be adequately secured and protected.

1.1 The purpose of the study

The purpose of this study was to assess the level of information security awareness at the GPAA, where information and records of members can be accessed, deleted or even lost. The question is whether the employees are aware of what information can be accessed, lost, stolen, or deleted and how to prevent a breach of security. The study will further assess the level of employee awareness of interventions such as continuous training, education and the awareness of information security.

1.2 The context of the study

The Minimum Information Security Standards (MISS) policy was approved and implemented during 1998. This policy is aimed at describing the minimum security standards and measures that all government departments should implement and consistently apply in order to protect sensitive state information (South Africa, 1998). In addition to MISS, the Department of Public Service and Administration (DPSA) issued the “Information and Communication Technology Security Guidelines” which all government departments are required to implement. In order to limit ICT security risks, the guidelines also require the following action plan to implement in security awareness:

- The development of a packaged security awareness program;
- The development of a workforce, training and awareness program; and
- The development of a policy and program for ISA and training.

The GPAA’s registry unit is the custodian of approximately two million files and documents. On the other hand, the GPAA receives documents through sources such as the Post Office, Client Liaison Officers (CLOs), and hand deliveries and through electronic channels from employers (within other government departments). This information needs to be recorded, processed and go through a value chain for the payment or finalisation of each case. This information, therefore, moves from one

person to another within the GPAA before a case is concluded. Regardless of whether there are documented standard operating procedures in place, this on its own is information security risk because some information may be lost, accessed by the wrong people and may have fraudulent activities take place.

1.3 Problem statement

GPAA has a training unit that focuses on product knowledge and the use of several functions in improving information management. However, based on a recent vulnerability assessment done by Ernst and Young on information security(GPAA, 2015), the outcome of the review indicates a regression on information security controls and its maturity. The study was a follow up on the maturity assessment. This study confirmed that although GPAA has a formal awareness and training program in place, and that specific user groups are trained during induction, there was a decrease in the level of maturity. The outcome of the assessment showed a decrease from a three (defined) rating to a two (managed) rating on awareness. One of the causal factors stated in the report was the absence of senior managers during information security training and awareness sessions.

These results further confirm that there are no consequences enforced on non-attendance of training and awareness sessions by employees. Further results indicated that although certain controls are in place to protect electronic data, these controls are not sufficient and could result in information security risks exposures. Other weaknesses identified include user access reviews, which were found to have reactive controls, instead of being proactive. These results indicate that there is less emphasis given to information security area to educate employees on the importance of safe custody of information.

The level of employee awareness of information security is currently unknown, which presents a problem when designing better information security training programmes, and preventing an accurate estimate of information security risks. This study will, therefore, assess the level of ISA based on the requirements contained in the Government MISS policy.

1.4 Objectives of the study

The main objective of the study was to establish the level of information security awareness in the GPAA and its alignment with the objectives set in the MISS Policy, procedures, and controls, including the awareness of tools and technology.

1.5 Research questions

The main research question which highlights the research problem and gives effect to the purpose of the study is: What is the level of information security awareness in GPAA?

In order to address this question effectively, it is broken down into the following specific questions:

- What is the level of awareness of the controls that are currently being utilised in the organisation such as passwords, use of emails and social networking?
- What is the level of awareness with relevant government policy interventions, such as Minimum Information Security Standards (MISS)?
- What is the level of awareness of the handling, transmitting and classification of records as required in the MISS Policy document?

1.6 The significance of the study

This study is significant because it will give the GPAA a starting point for managing information more effectively and efficiently based on the understanding of the employees' contribution to security issues. The aim of the study is to highlight and close gaps, which often result in information security breaches, by reviewing and implementing policies, procedures and processes. It will also assist the GPAA's training unit in their development of ISA manuals and awareness campaign packages to educate employees on the issues of handling members' information and records, and the consequences of non-compliance.

This study will also benefit other public entities and organs of state on information security management, and offer useful insights to decision makers and their stakeholders, to encourage further research on the topic.

1.7 Key theoretical concepts

Information: Information is regarded as any data that has been analysed and transformed into a meaningful and useful form (Van Der Westhuizen, Schellnack-kelly, & Geyer, 2010).

Security: Security is defined as implementing cost-effective measures, in order to reduce the probability or impact of loss-incurring events (F. Rogers, 2005).

Information security: Information security refers to an official organisational program aimed at applying security measures, to protect sensitive information.

Information security awareness: relates to an employee's knowledge and awareness of possible information security threats and issues, and their consequences, and how to address the related security incidents. (Bulgurcu, Cavusoglu, & Benbasat, 2010).

2. APPLICATION OF PRIOR RESEARCH

This chapter will review current discourse in the literature on the topics of the information security, existing policies and standards, and the role of human awareness.

In this digital age, the use of the internet has become second nature to millions of people. ICT has become central to the fulfilment of activities and tasks by people in their personal and work lives. Due to the high connectivity around the world and increased-reliance on ICT, organisations are increasingly facing new threats such as the vulnerability of data theft and loss of critical information (Qudaih, Bawazir, Usman, & Ibrahim, 2014). It is therefore essential for organisations to manage and improve information security to be competitive, maintain cash flow, be profitable and maintain a commercial image (ISO, 2005).

The global shift, characterised as a digital change by B. Von Solms (2006), has introduced major changes pertaining to information security governance. Companies within both the private and public sector have shifted their focus towards information security governance, by acquiring solutions that safeguard against unauthorised access to information and cyber threats. The importance of information security governance has become particularly important in the public sector because the

delivery of services has become more dependent on confidentiality, availability, and integrity of computer-based information and resources. According to Stephanou (2009), information security is about keeping information protected, safeguarding its integrity and privacy. Ngoepe (2008) argued that information management practice was the starting point for improved service delivery. Technical security measures and information security policies are crucial in achieving ISA and managing risks of security breaches.

Gemalto, a digital security company, conducted a study and released findings on breach level index. The results reveal that worldwide, almost 1.4 billion worth of data was compromised in 2016 (Istitute, 2017). Study results published by IBM security & Ponemon Institute study concluded that the cost of data breaches in South Africa is R32 million, a 12% increase as compared to 2016. These numbers reflect an increase in cyber threats and may have a negative impact, not only from a financial perspective but also from negative publicity, which could lead to low investor confidence.

2.1 Information security awareness

2.1.1 Introduction

Bulgurcu, Cavusoglu, and Benbasat (2009) define general information security awareness (GISA) an employee's knowledge and understanding of possible information security issues and their consequences, and how to address security incidents. De Maeyer (2007) on the other hand defined ISA "as an ongoing and organised effort that guides the behaviour and culture of organisations on security issues". These definitions highlight the human element and it is therefore evident that employees are central from both a knowledge and behavioural perspective.

Qing, Ng, and Kankanhalli (2007) held a view that programs on ISA are an important tool to educate users on preventing security incidents. Thomson (1999), advocated the notion that security awareness raises the value and importance of information and security procedures amongst users.Drevin, Kruger, and Steyn (2007) maintained that ISA is a form of deterrence, as it is aimed at reducing misuse of computers and human errors which may lead to theft and fraud.

The views held by the researchers are notably different, in that some believe that the aim of ISA is raising the level of awareness amongst the users of information, as a

deterrence to non-compliance, be it through awareness programs or other methods. Others are of the view that ISA is about users altering their behaviour and attitude towards information security.

In the past, information security solutions have primarily concentrated on technical countermeasures such as hardware, software, and networking systems to protect information in organisations (Spears & Barki, 2010). The research previously carried out on the aspect of information security concentrated on technical security measures, which support the functions of information security, i.e. confidentiality, integrity, and availability. With prior studies carried out, focusing on organisational measures such as procedures, tools, and methods on information nature, the use, and application of which may fail due to the lack of awareness. However, focusing only on technical features of information security is not sufficient as users may not comply with these measures (Siponen, 2001). These measures can be misused, misinterpreted or not used at all, therefore losing their usefulness.

A study by Merete Hagen, Albrechtsen, and Hovden (2008), found that awareness measures as compared to technical security measures are more effective, therefore practitioners should invest their efforts to achieve awareness and assess it regularly. These authors also remarked that there is a lack in theory and testable guidance, and approach on the subject matter to ensure that users commit and apply the relevant policies to achieve the information security mission, which may lead to frustration with security awareness efforts. There is a degree of work that was carried out on the topic of ISA; however, the majority of work is focused on the developing standards relating to knowledge and skill, and not specifically on human behaviour. Albrechtsen (2007) argued that even though information security procedures and guidelines are prescribed, users often fail to apply these guidelines. This was further supported by Aytes and Conolly (2003) who were of the view that there is limited published research on the aspect of human behaviour, with reference to information security.

An observation of prior research reveals that authors and researchers have focused on the importance of awareness initiatives and awareness techniques, describing steps or methods for implementing ISA(Vroom & von Solms, 2002).A study by Valentine (2006) also supported a similar organisation-specialised program.

Researchers also acknowledged the shortage of in-depth research on ISA interventions (Siponen, 2001).

2.1.2 Awareness of information security controls

According to Kruger, Drevin, and Steyn (2010), the success of the protection of information is dependent on the successful implementation of organisational information awareness plans and controls (p.316). These researchers regard authentication as a basic, yet imperative aspect of safeguarding information and data. Information security controls are divided into physical controls – i.e. office containing sensitive information to be kept locked at all time; technical controls e.g. user identity and passwords; and operational controls e.g. Human behaviour. Van Niekerk (2005) further advised that users need to be knowledgeable and educated about their roles in information security.

Burnett and Kleiman (2006) characterised three different ways of authentication; identity card, biometrics and use of passwords. The use of password is the most common authentication method, therefore organisations should exercise more caution as this method of authentication may be compromised.

Gross and Rosson (2007) argued that authorisation and authentication alone do not prevent or guarantee that information will not be accessed by authorised persons because the issue of social engineering remains.Wagner and Brooke (2007), supported this argument and further indicated that despite increased use of technical controls, there was still a failure to reduce the number of system attacks.

Butler and Butler (2014) conducted a study on the use of passwords by South African online consumers. From the study, only 23% of the users tested regularly change their passwords, with 70% indicating that although they are aware that it is a good practice, they do not change passwords regularly. The study concluded that South Africans considered convenience a higher priority over security and recommended that improvements via greater attention to the human computer interface and increased awareness, education and awareness programs.

Pretorius and Van Niekerk (2015) made recommendations when they discovered vulnerabilities in the South African industrial control systems as a result of user's insecure password management and outdated and uninstalled anti-virus and malware protection.

Organisations have to set up a system of defence so as to make it difficult for outsiders to reach company's assets and compromise them. Such a system refers to both practices that aim at training employees and guarantee them a safe behaviour on behalf of employees. During their daily routines, employees are not aware of the dangers and the negative impact on information systems they may have if they do not know security controls or they do not follow the company's security policies and procedures. There are also people outside the organisation that have the intention to harm the company assets, in order to gain advantages in future.

The studies and researches conducted as indicated above illustrate the need for awareness relating to control measures such as passwords, and controls around the use of emails to protect against sophisticated attacks such as phishing, and social engineering. These studies further illustrate how there can be a misalignment on information security knowledge, attitudes and behaviours. The objective of the study was therefore to assess the level awareness of GPAA employees.

2.1.3 Awareness of information security Policies and regulations

The literature contains many definitions of information security policy. According to Bulgurcu et al. (2010), an information security policy contains the roles and duties of employees on information security, ultimately aimed at protecting information and technology resources" (p.529). Information security policies, therefore, define appropriate and acceptable behaviours, which reduces the risk of human error and the rate of employee mistakes. The view expressed by Chen and Li (2014) is that information security policies are aimed at, reducing the misuse of computers and human errors which may lead to theft and fraud.R. Von Solms, Thomson, and Maninjwa (2011), highlighted the importance of implementing information security policies, which deter or mitigate information security related threats. These researchers also remarked that there is a need for organisations to implement these policies at a strategic, tactical and operational management level, in a form of standard procedures.

According to Bulgurcu et al. (2009), two factors drive employees to comply with requirements of information security policies, namely, "the employee's security awareness and their observed fairness of information security policy"(p.3). These researchers argued that employees should not view policies as punishment, but

rather as a countermeasure that helps to protect the organisation's assets. E. M. Rogers (2003) affirmed this view by promoting the view that attitude towards employees' compliance influences the decision by employees to adhere to the relevant IS policies. The purpose of ISA is, therefore, to raise the level of consciousness and to communicate the significance of information security, and the consequences if employees fail to adhere to policies and guidelines

ISA posits that a user understands information security policies, procedures and practices, and is able to use these measures when faced with potential security threats (Boyce & Jennings, 2002). The level of awareness amongst people should be increased; therefore, education and training should be used for the promotion of appropriate security behaviour within organisations. Information security standards, such as ISO/IEC27002 (2005) recommend that organisations use awareness campaigns to educate their employees on information security. Al-Awadi and Renaud (2007) also suggested that ISA should form part of information security implementation.

Laaksonen and Niemimaa (2011) conducted a study on information security policies and their effectiveness. Although ISA was not the main focus, it recommended that ISA should be taken into account when developing policies.

Every company should have established clear security policies and guidelines widely recognised and understood by employees. This will assist in order for management and employees to distinguish clearly the right attitude against the wrong. The study was to therefore assess the level of awareness amongst employees on their knowledge of the existing security policies, including the MISS applied at GPAA.

2.1.4 Awareness of information security – handling, transmitting and storage of information - Minimum information security standards

MISS prescribes minimum standards for handling and dealing with classified information. According to MISS, access to classified information should only be allowed to a person with the necessary security clearance, or a person authorised by the head of the department to view such information. Because government departments handle sensitive information, various security measures are mandatory. The "MISS" cabinet document (1998) sets out a range of measures to protect

classified information and prescribes security-vetting procedures that authorised persons should undergo security authentication. Every classification requires security measures for protection.

According to the MISS policy, documents are categorised and classified of a document or file is determined on its own merit based on the highest-graded information it contains. The first information category is “Restricted” and refers to information, if mishandled, or is handled by unauthorised people, may cause an inconvenience to the organisation or other individuals. The “Confidential”, classification, which is the next level, consists of information that, if handled or used without the mandatory clearance, may threaten the functions of the institution and individuals who perform such functions. “Secret” information refers to information, which if inappropriately disclosed, will threaten the institution. The “Top Secret” category refers to information, if disclosed, will cause damage to the institution. Employees with a “Top Secret” clearance, are required to sign a "Declaration of Secrecy" in order to guarantee control over the contents of such information or documents (Africa, 1998)

The MISS policy (1998) also requires that access to classified information, be limited to persons with a security clearance or who are authorised by the head of the institution. Access to these records should be in accordance with the appropriate level. The MISS Policy (1998) recommends that documents that are not in use must be safely stored as follows:

- *“*Restricted documents” - in a standard cabinet;
- “Confidential documents” - in secure cabinets;
- “Secret documents” - a special room with strong walls and strong door where valuable things are kept or secure cabinet’ and
- “Top secret documents” - in a strong room, safe or walk-in safe.

There is a need to protect sensitive information in government as it poses a risk to government department and the country. It can thus be concluded that government departments need to develop and implement security policies and programmes such as handling, transmitting and classification of records for the protection of information. The study was therefore to determine the level of employee awareness on knowledge when dealing with classified records.

2.2 Theoretical background and framework

Research on information security shows that, for information security implementation to be successful, it depends on both people and technology. Various studies provide proof that information awareness is a key direct and indirect factor that determines employee behaviour towards security compliance. In their study, Galvez and Guzman (2009), recognised that individuals with higher ISA practice higher/better ISA behaviour, therefore behaviour is key to information security compliance. Dinev and Hu (2007), also found that teaching users about possible risks of unsafe technologies influence individuals to adhere to security measures, and it encourages them to use protective information technologies for protection. Other researchers also support this view, for example, D'Arcy, Hovav, and Galletta (2009), who stated that 50 – 75% of information security instances emanates from within the organisation, therefore argued that awareness reduces risks and minimises security breaches, and also reduces intentional breaches, which result in punitive consequences.

D'Arcy et al. (2009) conducted a research and used the general deterrence theory, to show that implementing security awareness programmes i.e. education and awareness programs, installing counter surveillance and introducing IS security policies, results in the reduction of IT-misuse intention. The model advocates that awareness of information security controls can influence user perceptions on the possibility and consequences of sanctions linked to non-compliance and misuse.

Fishbein and Ajzen (1975) described ways of changing human beliefs, through active participation and influential communication. According to past literature, two theories are mentioned in information security when testing user behaviour, i.e. the Theory of planned behaviour (TPB), developed by Ajzen (1991) that suggests that the interaction with others influences your actions. Awareness in the context of information security consequently assists in developing a culture based on the promotion of good values and norms pertaining to information security.

The Protection Motivation Theory (PMT) on the other hand encourages individuals to act in a certain way and develop a specific behaviour. This research method was supported by Aytes and Conolly (2003) who held the view that making users aware of organisational policies and procedures relating to countermeasures influences and

motivates users to comply. Results on this theory based on several researchers have demonstrated that once users understand the significance of the role they play in information security, they are likely to change their behaviours and make conscious decisions.

Based on the preceding arguments, Table 1 below outlines the literature framework to get an integrated view relevant to the subject. For the purpose of the study, the framework provides an overview of concepts, implications, and recommendations alongside the applied theories type of behavioural outcomes, and methodology.

Table 1: an overview of ISA theoretical framework

Concept	Implication	Recommendation	Author/ Theory
Knowledge of ISA	General information security awareness (GISA) and information security policy awareness (ISPA) are key dimensions of ISA. ISA is a cognitive state of mind and educating users about probable risks and threats on technologies are influential in making them adhere to security measures	Users of IT should have the required knowledge to use information systems responsibly. ISA increases employees' reasoning and principles about information security and can result in employee's behavioural change.	TPB Bulgurcu et al. (2010)
	ISA is a cognitive and behavioural aspect. ISA is awareness of users	Employees should be aware of risks linked to information security, which	TPB Dinev and Hu (2007)

Concept	Implication	Recommendation	Author/ Theory
	and their interest in being knowledgeable about technical matters, and preventative strategies	should have a positive influence on employees' changed behaviour Making users aware and value the importance of ISA	Thomson (1999)
	ISA is a revealed in the behaviour of employees and is one of the information security behaviours.	ISA is viewed as 1 of the information security behaviours. ISA is an ongoing effort that guides behaviour and culture of the organisation	PMT theory Galvez and Guzman (2009) Spears and Barki (2010) De Maeyer (2007)
ISA – deterrence to IT misuse	Awareness reduces risks, minimise security breaches, & intentional breaches. ISA as a deterrence is aimed at reducing human errors (Intentional or unintentional), theft, fraud & misuse of computer assets.	Statement on awareness of security policy and guidelines, security education and training programs and monitoring of computer. ISA as an educational tool to alert users on preventative measures	• GDT • D'Arcy et al. (2009) • Drevin et al. (2007) • Qing et al. (2007)
Information Security	Attitude towards IS policies positively	ISA on policies reduces computer	• TPB Theory • Chen and Li (2014)

Concept	Implication	Recommendation	Author/ Theory
compliance	influences policy compliance intentions	abuse and information systems misuse.	• E. M. Rogers (2003) • (F. Rogers, 2005)
	IS policies are countermeasures that protect organisational information and technology assets.	Users should not view policies as punitive but as a motivation.	• PMT theory • Bulgurcu et al. (2010) • Bulgurcu et al. (2009)
	Implementing IS policies deters and mitigate IS related threats	IS policies should be implemented at strategic, tactical & operations management levels.	B. Von Solms (2006)
ISA Security controls – performance	Users should be knowledgeable & educated about security controls and the importance of protecting data	There is a significant association between ISA & information security behaviours.	• Bulgurcu et al. (2009)
	ISA positively influences attitude towards ISP compliance and indirectly via several belief factors.	ISA influences and forms favourable/unfavourable attitudes to employees' compliance with information security	• Bulgurcu et al. (2010) • Bulgurcu et al. (2009)

2.3 Previous consulting engagements and interventions

The GPAA has previously undertaken awareness and training programs, and a study on ISA satisfaction levels, with the aim of addressing the information security concerns. The information security policy was also revised and approved in 2014, in an attempt to improve on information guidance within the organisation. The policy is available on the GPAA intranet, for staff to access it and download. The attempts by the organisation are further enforced by senior management involvement, in that the senior managers regularly review security performance to ensure that the GPAA's security is effective and aligns with business goals.

The Information security business unit carried out campaigns during the 2017/18 financial year, through presentations and dialogue sessions. The statistics confirm that 164 employees attended these sessions and were trained on information security concepts such as "social engineering", "phishing" and "malware". With a staff complement of approximately 1200, only 13 %(164) attended these campaigns, and indicate a low level of attendance.

A study conducted by Ernst & Young in 2015 emphasised that although GPAA has a formal awareness and training program in place, there was a decrease in the level of information awareness amongst the staff as organisation decrease from a three (defined) rating to a two (managed) rating on awareness, which indicates a lack of maturity on the aspect. One of the root causes stated in the study was the lack of participation by senior management in the ISA campaigns, and there are no consequences for non-attendance. In their study, McFadzean, Ezingeard, and Birchall (2007) argued that senior management play a key role in effective security measures. The study identified a lack in senior management participation in information security awareness campaigns. The researchers argued that senior executives have a holistic view of the organisation and have the power to effect changes. The lack of participation within GPAA senior management could result in a negative impact on the level of awareness and effectiveness of ISA programmes carried out.

In 2017, the GPAA conducted a study in a form of a survey, to evaluate the level of satisfaction amongst staff on ISA campaigns. The results from the study as indicated

in Table 2 reflect that the overall satisfaction level was at 52%, indicating a good response. However, 18% of the respondents were dissatisfied and 30% were not positive. The results show that the aspect of awareness in GPAA requires urgent attention and that management needs to review how this awareness is implemented.

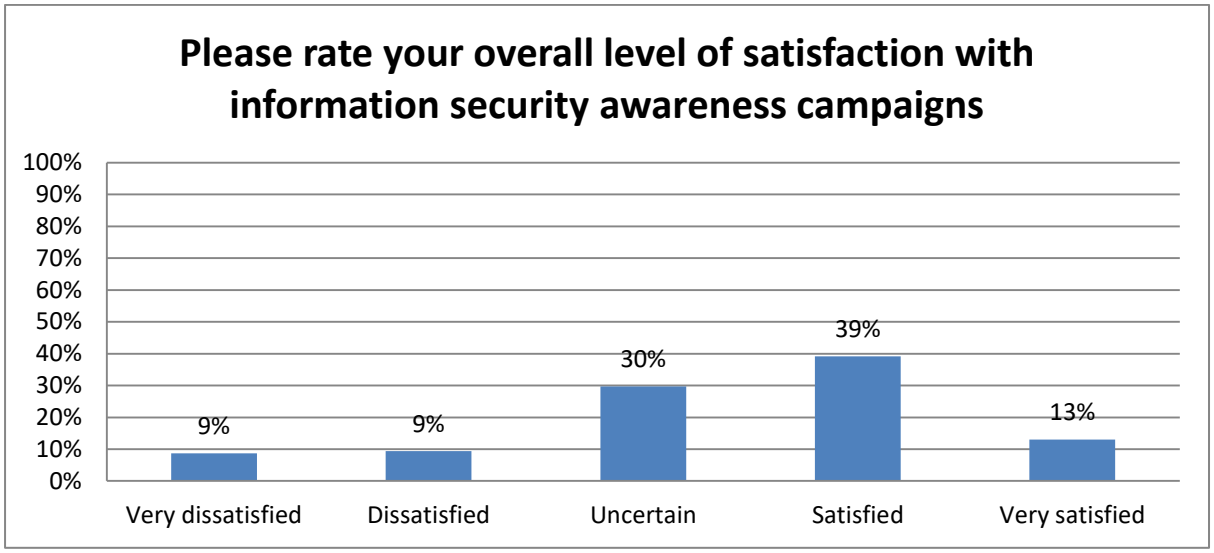


Table 2 - employee level of satisfaction with information security awareness campaigns

2.4 Summary

The MISS provides both general and specific guidelines for different documents and different staff positions. The effectiveness of the guidelines is dependent on whether people know them and put them to practice. It is unknown whether this is the case at the GPAA.

The literature review supports the argument that while organisations may have policies or guidelines on information security, it was very crucial to create awareness and measure effectiveness of information security. This study seeks to gain insights regarding the level of awareness of information security at the GPAA.

Previous researchers noticed that this was not the case in many organisations; therefore, it is possible that the level of awareness of the MISS policies would not be up to standard at the GPAA. The researchers also highlighted that the increase of the level of awareness may result in significant gains in the level of awareness(Johnson, 2006).

To test this proposition, the next chapter considers the methodology applied.

3. RESEARCH METHODOLOGY

The focus of this chapter is the research approach and method of the study, which includes the target population, data collection techniques, and the data analysis approach.

3.1 Research approach

The study used the quantitative model. The purpose of the quantitative approach was to provide answers to research questions. According to Sukamolson (2007), a quantitative method is a research tool which provides an explanation of occurrences through the collection and analysis of data using mathematical and statistical analytical methods (descriptive statistics). Bayat and Fox (2007) held a view that the use of numbers results in larger accuracy when reporting quantitative research results.

The researcher collected data using well-structured questions specific to the GPAA context, and thereafter, the data analysis of this study was performed quantitatively.

3.2 Research design

The nature of the study was exploratory rather than to test for hypothesis. The methodological approach was applied in a form of a survey study. The survey study makes use of structured questions as a data collection instrument. According to Babbie (2013), two survey designs models are available i.e. open-ended and close-ended questions. This study used close-ended questions were used on the survey questions, which the respondents were asked to make a selection from. The benefits of a structured survey include the speed by which the survey may be completed because of the minimal writing required, completion, analysis, accuracy and comparability of data. In this study, the researcher designed close-ended questions for ISA to gather data on the participants' perceptions.

An online survey was used for this study and consisted of four (4) sections and totalling 22 questions. These questions were used to respondents' level of awareness on various aspects of information security. The justification to using a survey method is that a similar study was conducted previously in assessing

information security awareness and proven to be beneficial and practical(Kruger et al., 2010).

The first part included five (5) questions that target personal information participant's gender, age range, educational level, employment category and the department/section they work in.

3.2.1 Knowledge of Policies and employee's responsibilities

A total number of seven (7) questions that tested the level of awareness of information security based on the requirements of MISS were included in the survey. These questions were linked to knowledge and awareness of Government legislation applicable to information security and the employees' responsibilities.

3.2.2 Employee behaviours and actions – handling, transmitting and classification of records

Seven (7) questions were also tested and the focus was to test application of the MISS document and ECT Act. These questions were scenario-based, which evaluated the respondents' action taken with information security content when handling, transmitting and their level of awareness on the classification of records.

Knowledge and consciousness of Information Security Policies

Based on the definition of ISA by Bulgurcu et al. (2010),two(2) the questions were included the survey that tested the respondent's level of awareness on GPAA's security and passwords policies existence, and also to test their level of consciousness when dealing with passwords.one(1) question was included in the survey and tested the respondent's level of awareness on security clearance, as required by MISS cabinet document.

3.3 Target population and sampling

3.3.1 Target population

Population refers to the theoretical specified combination of the elements in a study (Babbie, 2013). Similarly, Welman, Kruger, and Mitchell (2005) described the population as the total units of analysis, which the researcher intends to make specific conclusions about. The GPAA has 1200 employees which are the population for purpose of the study.

3.3.2 Sampling techniques

Given the small population size, and the researcher's anticipation that not all of the employees would respond to the survey request, the survey was distributed to all employees, thus the sample was equal to the full population. Certain job descriptions had an effect on the data collection because certain employees are cleaners, security officers, messengers, and maintenance, who do not have access to computers. Due to the data having been collected over a period of fourteen days, employees who were absent during this period could not partake. Emails were sent out to all GPAA employees via emails and all through global emails. All 1200 employees were covered and received emails on time. Participants were given 14 days to complete the survey. Participants were reminded once a week to complete and submit. After 14 days only 138 responses out of 1200 were returned which represents 11.5%. The major weakness to the study was the inability of a sizeable number of sample to complete the survey, which may have affected the results. This is a typical situation in social science research and also that despite the survey may not have covered all the problems sufficiently, those problems that were identified are valid and require urgent attention of the staff responsible for information security awareness.

3.4 Data collection methods

The researcher sourced all the relevant information by sending global emails to employees who have email access, enclosing the well-structured and easy to complete a survey, which allowed respondents to tick the preferred choices. The researcher administered the instrument and collected the responses after completion by the respondents.

3.5 Validity and reliability

This section describes the considerations relating to the validity and reliability of the research, taking into account the relevant internal and external aspects.

According to Leedy & Omrod (2010), the validity of a measurement instrument refers to the ability or extent to what you essentially intend to measure. This study aims to assess GPAA employee awareness of the minimum standards for handling and dealing with classified information as prescribed by MISS. The researcher tailored the survey in accordance with the guidelines set out in MISS, therefore ensuring correspondence of constructs and construct validity. The researcher also ensured that data collected was valid because the feedback received was mainly from users who had an encounter with information security awareness and educational campaigns within the GPAA environment and that the survey was based on research questions and this increased sampling validity, because despite some employees failed to respond, those who responded were well-qualified to provide information on the topic. The researcher ensured that the data collected had good construct validity by consulting government Acts, policies, GPAA reports on information security, legislation, previous theses relevant to the research questionnaires and objectives of the study. Comparison with the previous interventions for the improvement of information security awareness helped to ensure formative validity of the study.

The reliability of the research is determined by the quality of the analytical tool and its ability to produce the same consistent results (Babbie, 2013).Due to the limited duration of the study, test-retest reliability was not pursued. It was also not practical to introduce several questions testing the same concept because the employees had limited time and increasing the length of the survey could have negatively impacted the number of responses received. The researcher ensured that data collected through surveys was reliable using tests of variance and standard deviation: these measures helped to estimate internal validity of measures. In addition to that, the comparison between different population groups within the sample helped with understanding the reliability of particular measures on the level of the population as compared to the level of a population group.

3.6 Data Analysis

According to Struwig, Struwig, and Stead (2001), the analysis of data allows the researcher to interpret a large amount of data collected. This study used a data analysis in order to provide answers to research questions.

The quantitative data analysis method enables the researcher to interpret, describe and explain data using numeric and statistical means. According to Leedy and Ormrod (2010), the analysis of data involves the following steps: “(1) organization of details about the case; (2) classification of data; (3) interpret single occurrences; (4) identify patterns (5) synthesis and generalisations.”

The data captured by the researcher was statistically analysed to produce descriptive analysis results. Large data was reduced through the statistical analysis to summarize the frequency, range, mean and standard deviation of each data set. The study made use of tables and charts to display the frequency of responses and measures of dispersion for demographic questions in the survey. This study used the Likert scale as follows: (1) Strongly agree, (2) somewhat agree, (3) Neither agree nor disagree; (4) Somewhat disagree and (5) Strongly disagree. The research questions were answered according to the weighted average means. The Likert scale, therefore, establishes the extent of agreement or disagreement with statements resulting in the median, standard deviation and range of scores of variables as part of statistical analysis.

3.7 Ethical considerations

The GPAA granted approval to conduct research (Appendix B) and the following ethical issues were considered:

Voluntary participation: There were no potential consequences for those who chose not to participate, as the study was voluntary.

Confidentiality and Anonymity: The confidentiality of respondents was protected by excluding their names or identities.

The professional integrity of the researcher: It was the responsibility of the researcher to provide a comprehensive and accurate report, including methods used for data collection.

Recognition of participants' time and effort: Researchers ensured that they recognised the participants' for the time and effort given to this study.

The researcher adopted the above ethical considerations in order to assure the members of their participation.

3.8 Limitations

The following limitations are highlighted:

The commitment of the participants: The research participants may not show the full commitment to the study when required to give their full responses to the research questions.

Time: The time constraints on the part of the business school meant that the research would be conducted within a limited period.

Language: The interpretation of the language used is a potential barrier for some of the respondents to fully understand the survey. The researcher will have to provide clarifications to some questions posed to the respondents. A quantitative study is limited to the factors contained in the questionnaire thus a deeper understanding of the potential less tangible factors of organisational culture is not pursued. However, since the study intends to determine adherence to the guidelines of MISS, a quantitative assessment was more suitable as an assessment of the level of awareness and as a more actionable assessment.

4. DATA COLLECTION AND ANALYSIS

4.1 Introduction

This chapter analysed the data collected from the respondents and interpreted the relevant findings. The research used the quantitative approach to a strategy or mode of enquiry. The Statistical Package for Social Sciences (SPSS) version 25 software was used to analyse the survey responses and extract the necessary information. Information from respondents was collected using an online-survey obtained through qualtrics survey system. The aim of the survey was to establish the level of ISA at the GPAA, through the collection of data. The GPAA internal email portal circulated invitations through "general announcements".

There are approximately 1200 employees in the organisation, equating the population of 1200 for statistical purposes. 138 participants responded in total representing a total sample population of 138, therefore 11.5% of the organisation participated in the survey. The survey used a five-point Likert rating scale to obtain responses from participants. The Likert scale establishes the extent of agreement or disagreement with statements, designed to establish the responses' mean, standard deviation, and range of scores. In addition to the tabulated percentages of responses, the study used functionality within SPSS to show participants' level of awareness in their employment categories. This was important as it gave more indication of the category of respondents that require attention. The results are categorised into the following sections:

4.1.1 Demographics

The first part includes five (5) questions that target personal information participant's gender, age range, educational level, employment category and the department/section they work in.

4.1.2 Employee's level of awareness with relevant government policy interventions such as MISS and ECT Act

A total number of seven (7) questions that test the level awareness of information security policies were included in the survey. The survey questions were multi-choice based, with only one (1) possibly correct response. These questions were linked to knowledge and awareness of Governments legislation applicable to information security and their responsibilities. In order to determine the employees' level of awareness, establishing their knowledge of Minimum Information Security Standards (MISS) and electronic communications Act was key, therefore the respondents were asked about their understanding of processing, handling and transmitting sensitive information.

4.1.3 Employee's level of awareness in handling, transmitting, and classification of records

Seven (7) questions were included in the survey and were scenario-based questions, which evaluated the respondents' action taken with information security content when handling, transmitting and their level of awareness on the classification of records.

4.1.4 Level of awareness with a set of controls in place at the GPAA

The section refers to the second part of the definition of ISA by Bulgurcu et al. (2010), which is employees' awareness and knowledge of the ISA policies within the organisation. Three (3) questions referring to security programmes, use of passwords and security clearance were asked.

4.2 Information on demographics

4.2.1 Gender (Q1)

Table 3 - Gender Breakdown of the respondents

#	Answer	Frequency	Percentage
1	Male	55	39.86%
2	Female	83	60.14%
	Total	138	100%

Table 3 reflects that just over 80 of the respondents were females and over 50 were males. These figures are in line with the demographics of GPAA staff on the staff establishment and the trend within the organisation. The study, therefore, established the awareness mean score of the GPAA population and compared it to the gender groups. In total, it is seen that the mean score is higher in all statements because the number of females exceeded the male count (Appendix C).

4.2.2 Age range (Q2)

Table 4 - Age Range of respondents

Age Range of participants	Frequency	Percentage
15 - 25	3	2.17%
26 - 35	43	31.16%
36 - 45	51	36.96%
45 and above	41	29.71%
Total	**138**	**100%**

Data related to the age range of respondents was collected and tabulated as presented in Table 4. The highest number was on respondents between age 36 – 45 years which shows (36.96%), followed by 26 – 35 years (31.16%) and 29, 71% were above 45 years of age and just above 2% were 25 years and younger. A similar test was used for observing the difference between ages as that used in the previous example about gender, and the tests do not indicate much of the difference. The measure of awareness is not significantly different amongst groups considered in all the questions (Appendix E).

4.2.3 Highest Education Level attained (Q3)

Education can play an important role where awareness is concerned about importation security matters. Table 5 below indicates the education level of the respondents:

Table 5 - Highest level of education attained

#	Answer	Frequency	Percentage
1	None	0	0.00%
2	Grade 1 up to Grade 7	0	0.00%
3	high School	38	27.54%
4	Undergraduate	53	38.41%
5	Postgraduate	47	34.06%
	Total	**138**	**100%**

A noticeable number (38.41%) of the respondents have an undergraduate qualification, and just above a third (34.06%) have a postgraduate qualification and just above a quarter (27.54%) a high school qualification.

4.2.4 Employment Category (Q4)

Table 6 - Employment Category

#	Answer	Frequency	Percentage
1	Clerical	5	3.62%
2	Admin	63	45.65%
3	Junior	50	36.23%
4	Senior management	19	13.77%
5	executive	1	0.72%
	Total	138	100%

Table 6 presents the demographics of the employment categories of participants. A noticeable number (45.65%) of the respondents were people who did administration work in the organisation and just more than a third (36.23%) were in junior roles, 13.77% were in senior management and an insignificant number were executive management and 3.62% were doing clerical work. As stated in the study conducted by McFadzean et al. (2007),senior management play a key role in effective security measures. 13.77% of senior management with only 1 executive member completing the survey indicates a lack of participation by this level. This may in future result in a negative impact on the culture of the organisation and level of awareness on ISA programmes that are carried out.

4.2.5 Name of Department (Q5)

The respondents were from different departments within the organisation known as Programmes. The Programmes are divided between core business and support services.

Table 7 - Name of Department (Programme)

#	Answer	Frequency	Percentage
1	Programme 1.1 - Support Services	30	21.74%
2	Programme 1.2 – Finance	18	13.04%
3	Programme 1.3 – Governance	17	12.32%
4	Programme 2.1 - Employee Benefits	30	21.74%
5	Programme 2.2 - National Treasury	12	8.70%
6	Programme 2.3 - Client Relations Management	31	22.46%
	Total	**138**	**100%**

Just more than half (53%) of the respondents were from core business i.e. Programme 2 and the remaining 47% was from support services i.e. Programme 1. This was important because of the employees in Programme 2 deal with personal client information, and as a result, there was a risk of the information security being compromised.

4.3 Information security awareness questions - Q 6 to Q22

Table 8 presents the overall summary of the three measures of dispersion as extracted on SPSS, the mean, standard deviation, and variances. Most respondents showed a perceived high level of ISA. The lowest Mean score rating shown in Table 8 is 3.32 with the highest scores of 1.26. The level of awareness of information security at the GPAA is perceived a high. For example, the question of ISA knowledge of passwords (Q8) suggests that respondents are highly aware of the level of importance of this control measure. Although the lowest scores Q20 and Q22, with lowest Mean scores of 3.20 and 3.34 respectively, the results suggest improvements in the areas of record keeping and security vetting. Observations on the variance analysis also indicate a low difference between the observed score with a few exceptions in Q20, Q21 & Q22 showing a spread of scores by participants.

Table 8 - Descriptive Statistics

	Survey questions	N	Range	Min	Max	Mean	Std. Deviation	Variance
Q6	I have a firm knowledge of legislation applicable to information security in Government institutions i.e. “MISS Policy” and Electronic Communications Telecoms Act	138	4	1	5	2.32	1.067	1.138
Q7	Familiarity with the GPAA's Information Security Policies & responsibilities as an employee	138	4	1	5	1.82	.822	.675
Q8	I understand the requirements for and use of strong passwords.	138	3	1	4	1.26	.620	.384
Q9	I know and understand the term " social engineering" Phishing" and " Cyber Crime"	138	4	1	5	2.04	1.117	1.247
Q10	I know how to protect against “social engineering” “phishing” and “cybercrime”.	138	4	1	5	2.33	1.155	1.333
Q11	I know when and who to contact if I am suspicious of any information security incident/threat.	138	4	1	5	1.85	.988	.977
Q12	I always lock my system when I move away from my computer and use a password-protected screensaver.	138	4	1	5	1.46	.881	.776
Q13	I understand what information is considered “sensitive” “classified” at the GPAA	138	4	1	5	1.56	.837	.701

	Survey questions	N	Range	Min	Max	Mean	Std. Deviation	Variance
Q14	Documents containing sensitive information are classified according to their levels of classification (Restricted, Confidential, and Top Secret) at the GPAA.	138	4	1	5	1.90	1.062	1.128
Q15	I am aware of course materials, security manuals and posters on information security, available at the GPAA, and know how to access them.	138	4	1	5	2.16	1.116	1.244
Q16	I understand the requirements and methods used for transferring, storing, labelling and handling sensitive information at the GPAA.	138	4	1	5	2.09	1.091	1.189
Q17	I am familiar with security programmes for staff at the GPAA to be security conscious on the protection of Information security.	138	4	1	5	2.08	1.040	1.081
Q18	I do not leave sensitive data unattended in open areas (i.e. Copiers, Desks, and Faxes).	138	4	1	5	1.60	.940	.884
Q19	GPAA systems do not allow unauthorised access to information of records.	138	4	1	5	1.79	.985	.970
Q20	GPAA member records can be removed without authority from their premises.	138	4	1	5	3.34	1.497	2.241

	Survey questions	N	Range	Min	Max	Mean	Std. Deviation	Variance
Q21	All employees handling sensitive information have valid security clearance certificates.	138	4	1	5	2.67	1.245	1.550
Q22	I see actions pertaining to information security as an irritant rather assisting in securing information in the organisation.	138	4	1	5	3.20	1.405	1.973

The next set of questions tried to identify the respondents' level of ISA and to establish if they have the knowledge to protect information.

4.3.1 I have a firm knowledge of legislation applicable to information security in Government institutions i.e. "MISS Policy" and Electronic Communications Telecoms Act (Q6)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	33	23.9	23.9
2	Somewhat agree	52	37.7	61.6
3	Neither agree nor disagree	35	25.4	87.0
4	Somewhat disagree	12	8.7	95.7
5	Strongly disagree	6	4.3	100.0
	Total	**138**	**100.0**	

Table 9 - Knowledge of MISS & ECT Act

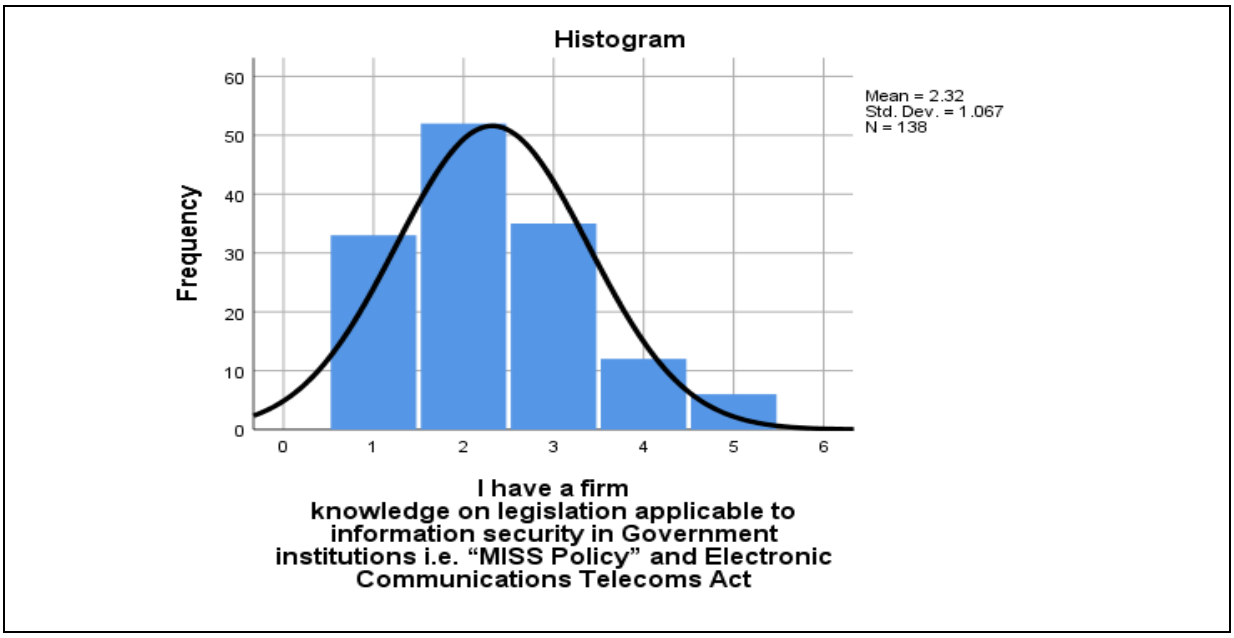


Figure 1 - Knowledge of MISS & ECT Act

Table 9 and figure 1 indicate that 61.6% of the respondents agreed that they have a firm knowledge on legislation applicable to information security in Government institutions i.e. "MISS Policy" and Electronic Communications Telecoms Act, 13.05% disagreed and a quarter (25.4%) neither agreed nor agreed. The quarter that neither agree nor disagree, present a potential challenge, which may be interpreted into a lack of awareness on Government policies such as the "MISS" policy and "Electronic Communications Telecoms Act".

Participants who neither agreed nor disagreed were largely at admin and junior level, which reflects 25.4%.The mean as calculated reflects 2.32 (figure 1) which specifies that the average scoring was agreeable to the statement. The 13% of respondents that disagreed with the question are from the same employment category, clerical, admin and junior level (Appendix D). The rest of the levels agreed with the statement. This view suggests that, even though there was an overall high level of awareness on knowledge of legislation applicable to information security, the demographics indicate that it was only at certain employment category levels, and this could be due to a number of issues i.e. insufficient awareness of the relevant legislation, or communication barriers within the organisation. Based on the level that are not aware the potential risk is that they were not familiar with the policies and

procedures because they were either not involved in the development of such policies and procedures, or the developed policies have not yet been presented to all employees.

While knowledge of IS policies mean values are similar for all age ranges, employees of Age range 15-25 and 26 -35 have high mean values (Appendix E), while the Age group of 45 and above scored the lowest values (2.17) for the knowledge of policies that exists at GPAA.The results demonstrate, although it cannot be proven that, with the increase in age, mean values improve, indicating increased level of awareness as they grow.

According to Morgan and Boardman (2012) it is good practice for Government Departments to adopt written policies that set out principles and procedures that will ensure compliance with government legislations i.e. MISS and ECT Act.

Without knowledge of these policies, procedures or guidelines, employees may misuse, misinterpret or ignore security related procedures and these policies and procedures could lose their real usefulness. Increased awareness also minimises security related faults. Based on the results reflected above, more attention and efforts should be placed on educating and creating awareness to staff at an admin, clerical and junior level, with a particular age range of 15 – 35.

4.3.2 I am familiar with the GPAA's Information Security Policies and my responsibilities as an employee (Q7)

Familiarity with the organisation's information security policies and the employee's responsibility is of utmost importance. Table 10 reflects the following views by respondents:

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	52	37.7	37.7
2	Somewhat agree	66	47.8	85.5
3	Neither agree nor disagree	15	10.9	96.4
	Somewhat disagree	3	2.2	98.6
4	Strongly disagree	2	1.4	100.0
5	Total	138	100.0	

Table 10 - Knowledge of policies & employee responsibilities

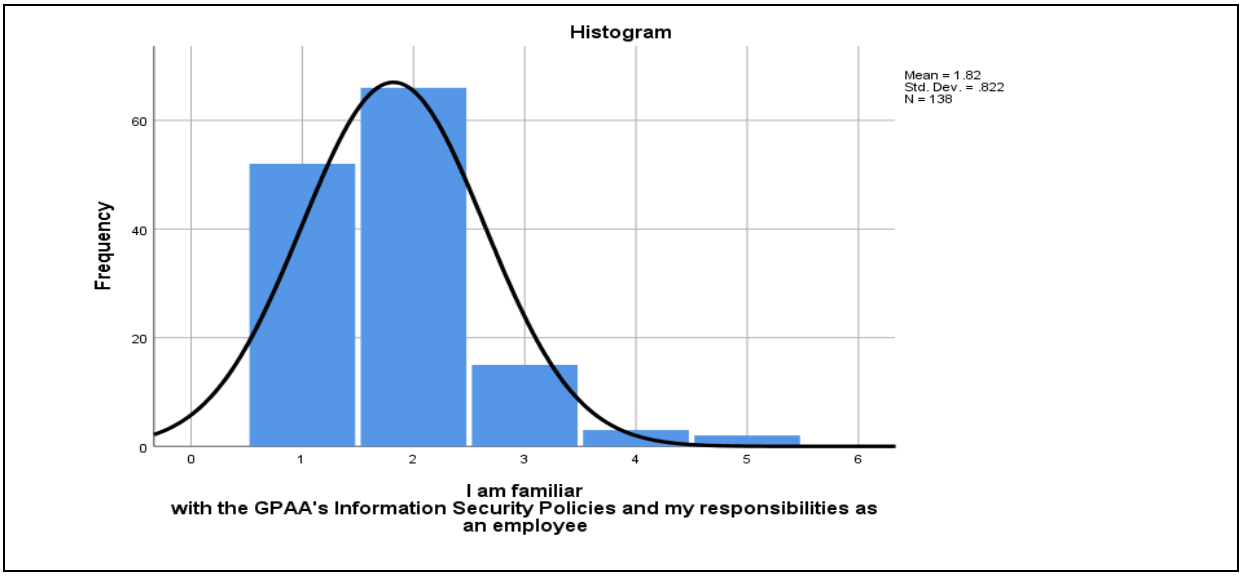


Figure 2 - Knowledge of policies & employee responsibilities

Table 10 and figure 2 above indicate that a majority, 85.5% of the respondents have knowledge of information security policy and understand the responsibility of the employees in the organisation, less than 5% disagreed and 10% neither agreed nor disagreed. The calculated mean of 1.82(figure 2), suggests a perceived high level of awareness on respondents' familiarity with their responsibilities relating to information security. The 10% that neither agreed nor disagreed were from both from admin and junior level (Appendix D).

The comparison between the two questions (Q6 and Q7) and the feedback received from response suggests that even though employees are familiar with IS Policies (85%), only 61% have firm knowledge of IS Policies in government. According to definition of ISA by Bulgurcu et al. (2010) Information security awareness is about knowledge and understanding possible information security issues and how to address their consequences.

The outcome of the survey therefore indicate that although respondents have higher level of awareness on being familiar with GPAA policies, the do not have as much knowledge of the contents of government IS policies such as MISS and ECT Act. This is a concern as the respondents may not adhere to policy requirements when dealing with IS matters, and information may be compromised. The results also

indicate a gap in development of IS policies and user awareness on IS, as indicated in the study by Laaksonen and Niemimaa (2011), who recommended that information security awareness should form part information security policy development.

A similar trend was observed on the Age range as in the previous results, with higher mean values at age range between 15 – 25 and 16 – 35(Appendix E) .All employees with age range above 35 years scored lowest (1.88).

4.3.3 I always lock my system when I move away from my computer and use a password protected screensaver (Q8)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	99	71.7	71.7
2	Somewhat agree	23	16.7	88.4
3	Neither agree nor disagree	9	6.5	94.9
4	Somewhat disagree	5	3.6	98.6
5	Strongly disagree	2	1.4	100.0
	Total	138	100.0	

Table 11 - Locking of computers to prevent unauthorised access

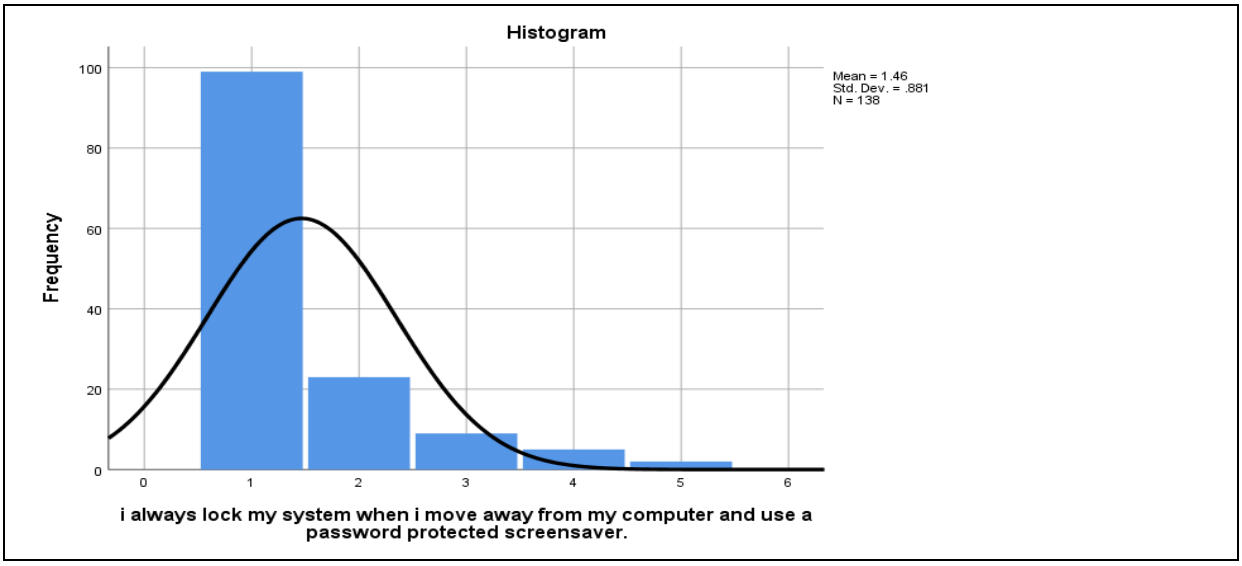


Figure 3 - Locking of computers to prevent unauthorised access

One of the controls of information security is that employees should lock their computers to prevent unauthorised access to their computers. Table 11 indicate the

level of information consciousness when taking precautionary measures on securing information on their computers against unauthorised access. The majority (88.41%) of respondents strongly agreed and somewhat agreed that they always lock their system when they move away from their computer and use a password protected screensaver. With a mean score of 1.46 (Figure 3), this strongly suggests that there is a high level of awareness. Only 5% strongly disagreed or somehow disagreed whilst 6.5% neither agreed nor disagreed with the statement of locking their computers and using password protected screensaver. These exceptions of 5% and 6.5% are from the junior and admin employment category (Appendix D), reflecting a low level of awareness on that limited number of participants.

It is also noteworthy that out of 103 participants belonging to both the junior and admin category, only 6 of the respondents disagree on their response, which indicates a small margin of disagreement. The results also demonstrates similar trends with the previous statement regarding knowledge of policies and their responsibilities as employees, and confirms the definition by Bulgurcu et al. (2009), on information security awareness.

Deterring IS misuse can be achieved by using both technical controls such as monitoring software, use of strong passwords. It is therefore critical that all employees, irrespective of their levels to know and understand the usage of technical controls, that will assist as a deterrence to security risks.

4.3.4 I understand the requirements for and use of strong passwords (Q9)

Table 12 - Use of strong passwords

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	114	82.6	82.61
2	Somewhat agree	13	9.42	92.03
3	Neither agree nor disagree	10	7.25	99.28
4				
5	Somewhat disagree	1	.72	100.0
	Total	138	100.0	

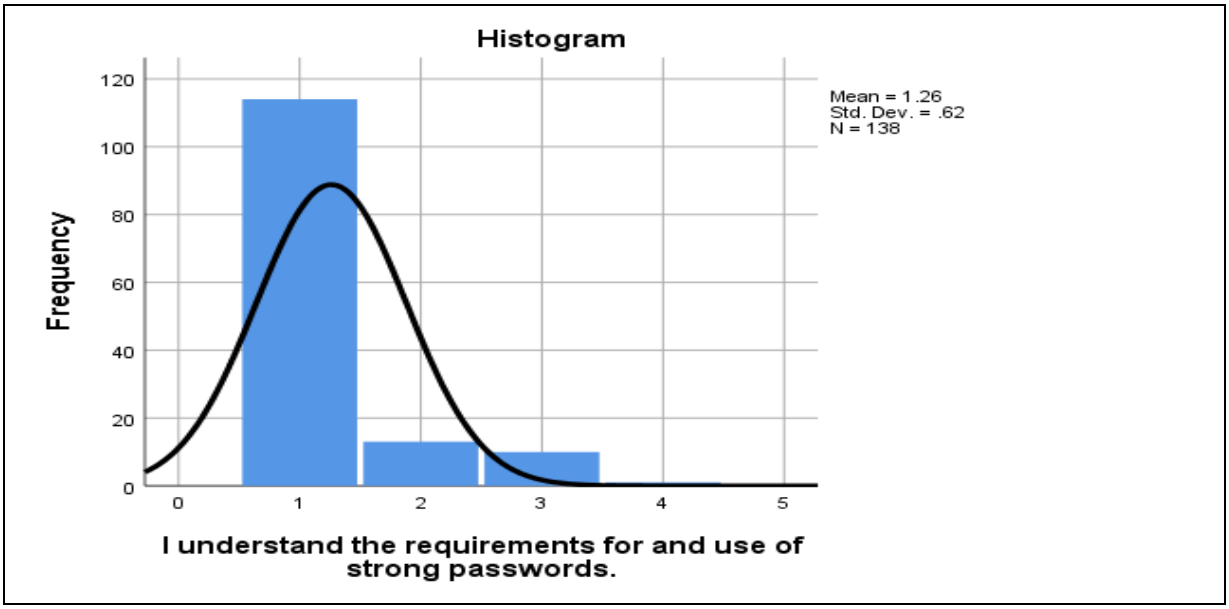


Figure 4 - Use of strong passwords

The use passwords are one of the controls for information security. Table 12 and Figure 4 indicate the views of the respondents on the use of strong passwords as a control to protect information.

Almost all the respondents 92.0%(Table 12) indicated that they understand the requirements for, use of strong passwords, only 7.2% neither agreed nor disagreed, and only 0.7% was neutral. The mean score of 1.26 (figure 4) also confirms a high level of awareness. The results from participants indicate a perceived high level of knowledge on the use of strong passwords. Three categories, clerical, admin, and junior had a small number of participants, disagreeing with the statement (Appendix D).

These results are consistent with the responses on Question 9(use of password protected screensaver). The results also reflect a low level of awareness in the admin, junior and clerical level.

4.3.5 I know and understand the term “social engineering" Phishing" and “Cyber Crime" (Q10)

Table 13 and figure 5 below indicate the views of the respondents on their knowledge and understanding of some of information security terms, namely “social engineering" Phishing" and “Cyber Crime".

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	53	38.4	38.4
2	Somewhat agree	50	36.2	74.6
3	Neither agree nor disagree	19	13.8	88.4
4	Somewhat disagree	9	6.5	94.9
5	Strongly disagree	7	5.1	100.0
	Total	138	100.0	

Table 13 - Knowledge & understanding of terms

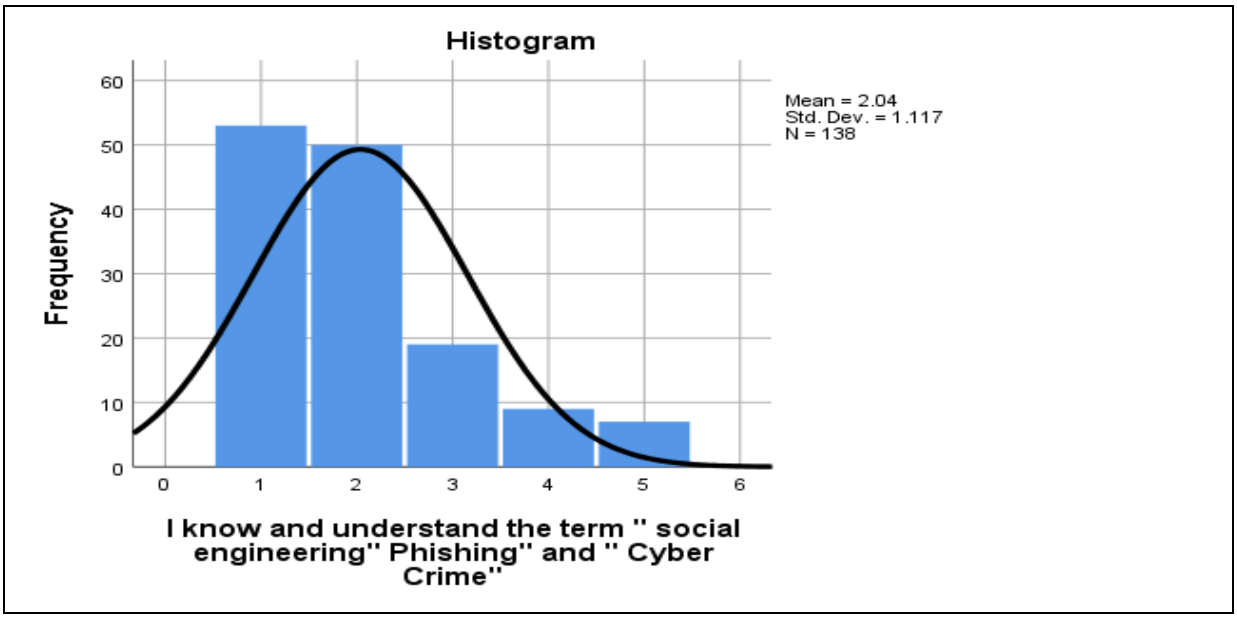


Figure 5 - Knowledge & understanding of terms

Based on the results reflected in Table 13 and Figure 5, the majority of respondents 74.6% agreed that they know and understand the terms term “social engineering" “Phishing" and “Cyber Crime, meanwhile 11.6% disagreed and 13.8% neither agreed nor disagreed. This was another indication of a high level of awareness with a mean score of 2.04(figure 5). 11.6% represented a small percentage of respondents in the category of clerical, junior and admin. The same categories, although small have neither agreed nor disagreed, with 13.7%.

Despite these results being low percentages in disagreements (11.6%), these categories of employees handle confidential records on a regular basis and may

subject the organisation to information security attacks/breaches. The study by Dinev and Hu (2007) indicates that teaching users about possible risks of unsafe technologies influence individuals to adhere to security measures. It is therefore important that respondents who were neutral and also disagreed to the question obtain the necessary awareness on information security. Awareness efforts targeted to those employees that are neutral will help prevent the organisation from potential exposure to breaches as outlined in the study by D'Arcy et al. (2009).

4.3.6 I know how to protect against "social engineering", "phishing" and "cybercrime" (Q11)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	34	24.6	24.6
2	Somewhat agree	54	39.1	63.8
3	Neither agree nor disagree	32	23.2	87.0
4	Somewhat disagree	6	4.3	91.3
5	Strongly disagree	12	8.7	100.0
	Total	138	100.0	

Table 14 - IS Knowledge: how to protect against IS threats

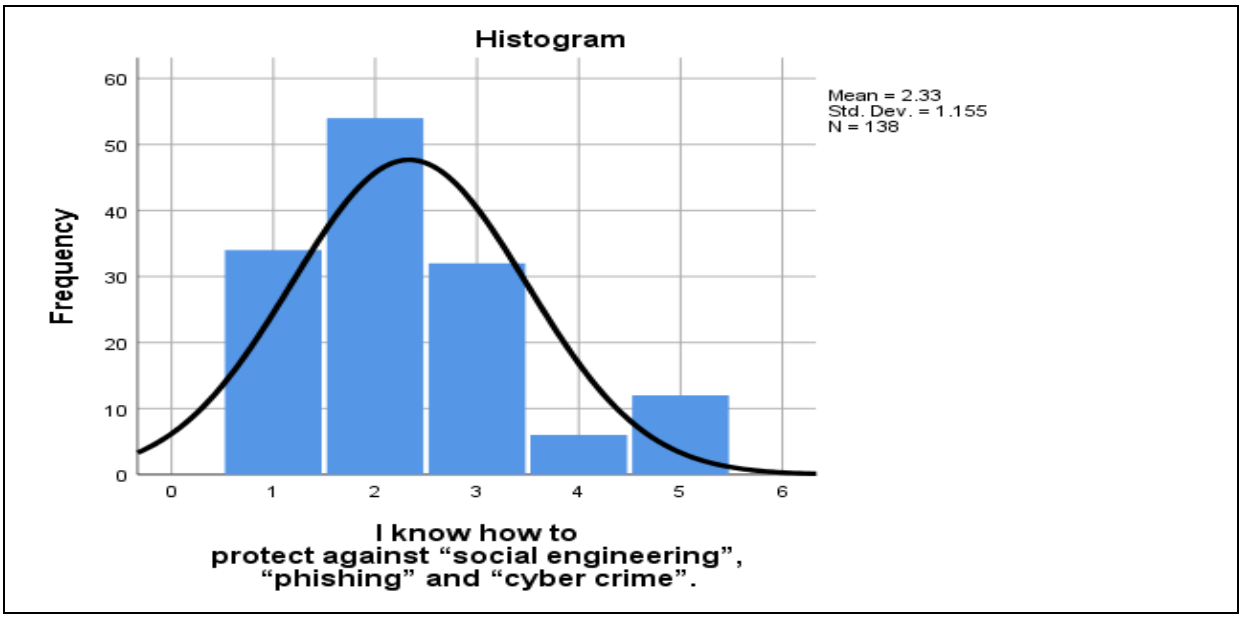


Figure 6 - Knowledge to protect against IS threats

Table 14 and Figure 6 indicate that 63.8% of the respondents agreed that they know how to protect against social engineering", "phishing, "cybercrime" .13% disagreed, and 23.2% neither agreed nor disagreed. Although there was almost a majority that agreed to the statement (63.8% and a mean score of 2.33), the respondents who could not agree nor disagree present a potential risk in that, they may not know how to respond to any threat of information and this could comprise the organisation's assets.

On the participants who did not agree with the statement (13%), although small, they also present a potential problem similar to the participants who were neutral. Surprisingly, 1 executive participant did not agree nor disagree with the statement. 13% of the participants that disagreed include senior managers. Of the 19 senior managers that participated, although the majority agreed with the statement, 2 were neutral and 1 disagreed with the statement (Appendix D).

Surprisingly, when comparing results obtained in Question 10 and Question 11, even though 74.6% of the respondents agreed that they know information security concepts such as "Phishing", "Social Engineering" and "Cyber-crime", only 63% know how to protect against information security attacks. These results indicate that there is high level of awareness on knowledge of IS concepts, but may not be able to apply any controls and protect organisation assets against any malicious attack.

Senior Managers who were neutral and disagreed to the statement indicate that there is a lack in top management's role in advocating ISA and also reflect that there is lack of knowledge in dealing with risks relating to threats and incidents that may cause damage to the organisation. These potential risks also apply to other categories of employees who may fall victim to threats and attacks.

4.3.7 I know when and who to contact if I am suspicious of any information security incident/threat (Q12)

Employees should know when and who to contact if they observe suspicious information security incident or threat; their views are reflected below:

Table 15 - knowledge of when and who to contact

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	62	44.9	44.9
2	Somewhat agree	49	35.5	80.4
3	Neither agree nor disagree	16	11.6	92.0
4	Somewhat disagree	8	5.8	97.8
5	Strongly disagree	3	2.2	100.0
	Total	138	100.0	

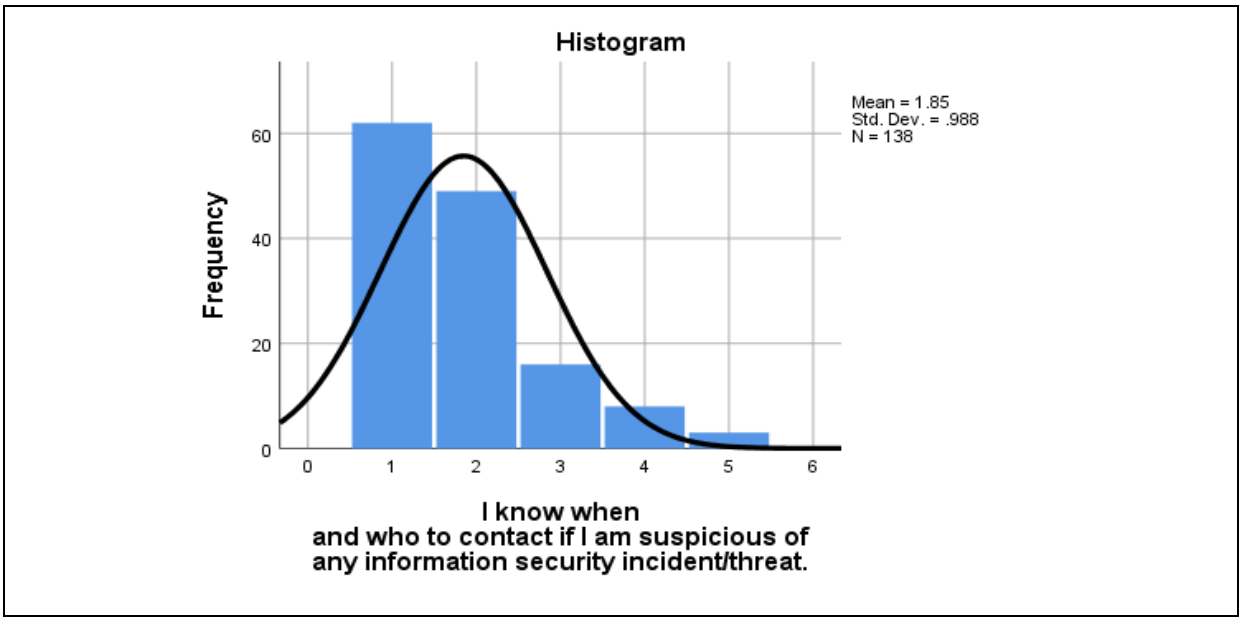


Figure 7 - Knowledge of when & who to contact

The statement above emphasises the significance of knowing whom to contact in the event of a security incident. The majority (80.4%) of the respondents agreed, only 8% disagreed and 11.6% neither agreed nor disagreed. The feedback in this question stated that they knew when and who to contact. If employees do not know whom to contact, many incidents or events can happen and go undetected or unrecognised, and the organisation may incorrectly view itself as a safe environment. The 80.4% is a good indication that participants know when and who to contact if faced with IS threats. 1 in senior management disagreed with the statement, together with other junior staff, Admin, and clerical staff (Appendix D).

The results on this question when compared to Question 11 above indicate that, although a lesser number of respondents (63%) know how to deal or address potential threats of “Phishing” “Social engineering” and “cyber-crime”, 80.4% know who to contact when they suspect a security incident. This presents a mitigation strategy by those employees who do not know how to deal with potential IS related threats (Table 15).

4.3.8 I understand what information is considered “sensitive” or “classified” at the GPAA (Q13)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	83	60.1	60.1
2	Somewhat agree	41	29.7	89.9
3	Neither agree nor disagree	7	5.1	94.9
4	Somewhat disagree	6	4.3	99.3
5	Strongly disagree	1	0.7	100.0
	Total	138	100.0	

Table 16 - Knowledge of sensitive and classified data

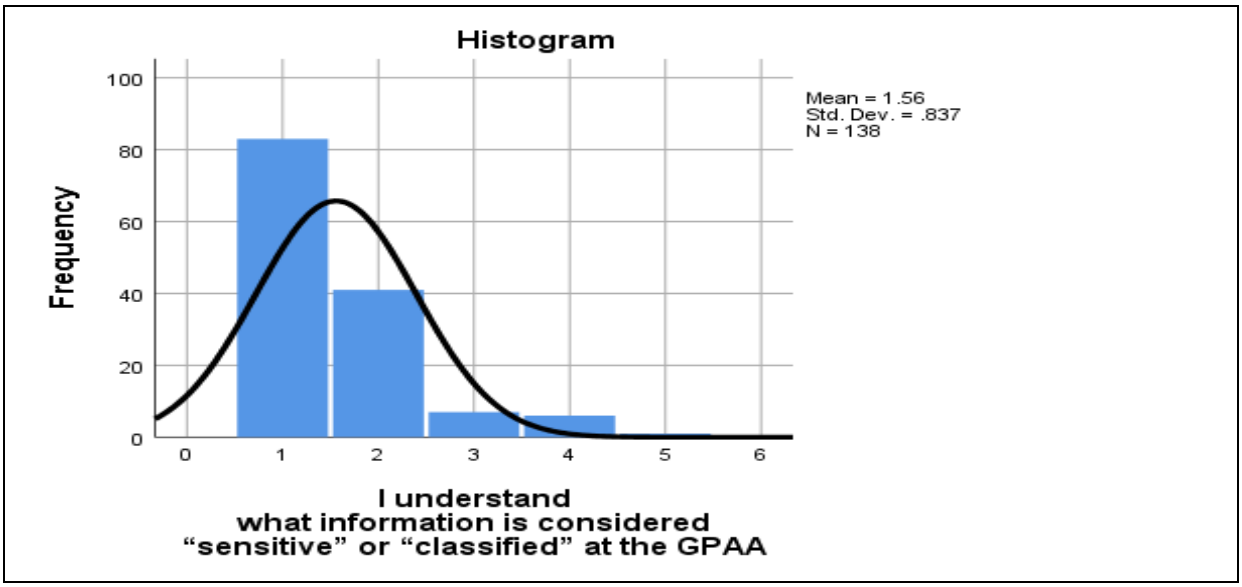


Figure 8 - Knowledge of sensitive & classified data

According to information security measures, information must be classified and only employees vetted can handle the type of information they are vetted for. In the statement “I know and understand information that is considered sensitive and classified, the majority of responses were between “strongly agree” and “somewhat

agree" (89.9%). A very small percentage of respondents were neutral (5%) and disagreed (5%). This represents a perceived high level of awareness on information security. Admin and junior categories (5%) have disagreed with the statement, and 1 senior manager (Appendix D).

4.3.9 Documents containing sensitive information are classified according to their levels of classification (Restricted, Confidential, and Top Secret) at the GPAA (Q14)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	64	46.4	46.4
2	Somewhat agree	41	29.7	76.1
3	Neither agree nor disagree	20	14.5	90.6
4	Somewhat disagree	9	6.5	97.1
5	Strongly disagree	4	2.9	100.0
	Total	138	100.0	

Table 17 - Classification of records

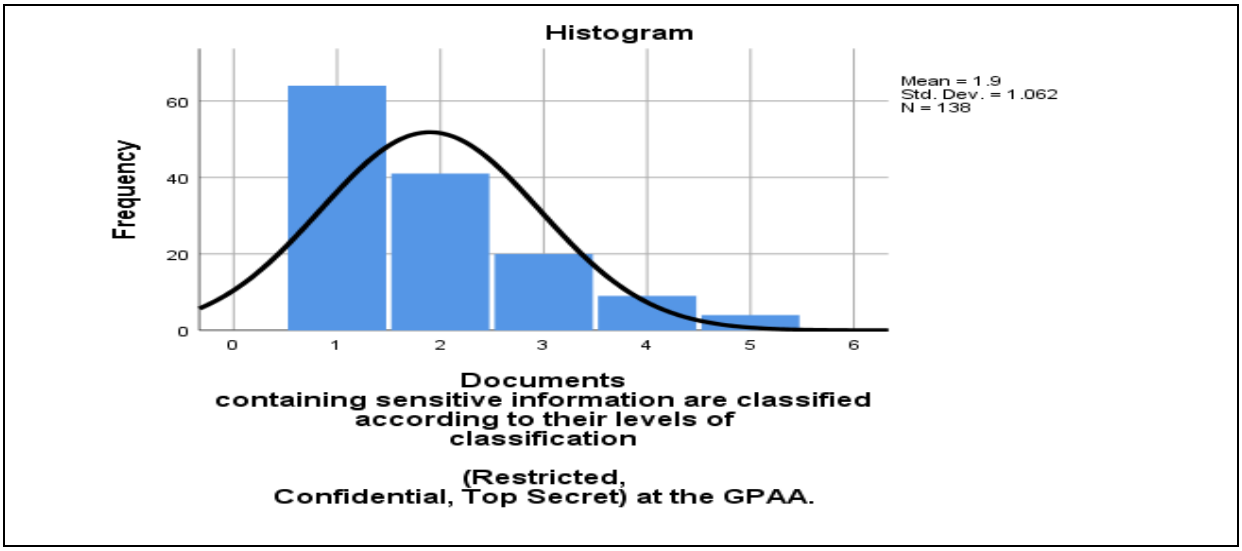


Figure 9 - Classification of records

Table 17 and Figure 9 indicate the views of employees regarding the classification of information in GPAA. The majority (76.1%) of the respondents agreed that documents containing sensitive information are classified according to their levels of classification (Restricted, Confidential, Top Secret) at the GPAA, meanwhile only

9.4% disagreed and 14.5% neither agreed nor disagreed. Surprisingly, of the 14.5% of participants that disagreed, a small percentage was from both senior management (2) and executive (Appendix D).

When comparing results obtained on this question (Q14) and the results presented in Q13 above, there is a concern that, even though employees have knowledge of what information is regarded as sensitive (89.9%), only 76.1% agreed to the company's practice of classification of records in line with MISS.The results indicate a low level of awareness on records that are classified in the company. In addition to that, from the 14.5% that disagreed, 2 senior managers also disagreed with the statement, posing a lack of awareness on the application of the MISS policy by all levels, including at senior management level.

4.3.10 I am aware of course materials, security manuals and posters on information security, available at the GPAA, and know how to access them (Q15)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	46	33.3	33.3
2	Somewhat agree	48	34.8	68.1
3	Neither agree nor disagree	26	18.8	86.9
4	Somewhat disagree	12	8.7	95.6
5	Strongly disagree	6	4.4	100.0
	Total	138	100.0	

Table 18 - Awareness of information security material

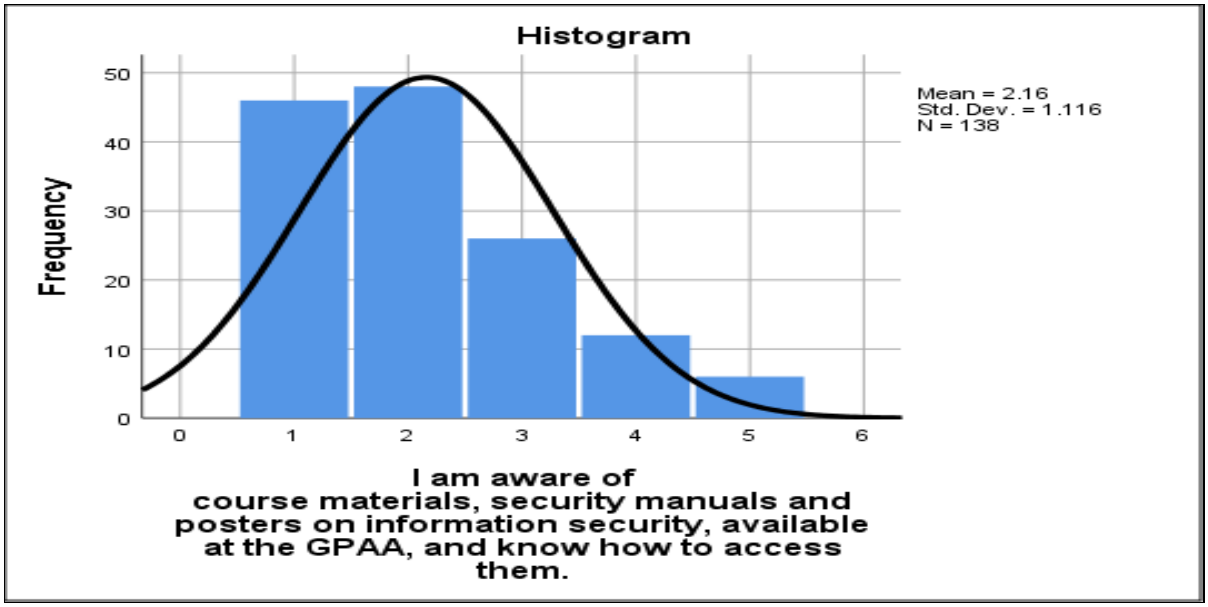


Figure 10 - Awareness of information security material

Table 18 and figure 10 indicates 68.1% respondents that agreed that they are aware of course materials, security manuals and posters on information security, available at the GPAA, and know how to access them (15) and 13.1% disagreed and 18.8% neither agreed nor disagreed. With a mean of 2.16(Figure 10), the results do indicate an observed high level of awareness on the use of promotional items used to educate employees about information security. Respondents who disagreed and were neutral on the statement are from admin and junior positions (Appendix D).

18.8 %(26) of the respondents who were neutral is a concern, and can also be linked to the results of previous engagements and consulting activities at the GPAA. One of the contributing factors to their lack of awareness in previous engagement was that materials relating to information security were not easily accessible by these employees, which prevented them from being aware of existence of information security materials.

Linking this question and feedback on the previous question relating to knowledge of information security policies such as MISS and ECT Act above (Q6), there appears to be a level of consistency on how employees responded to this question. A similar trend was observed in that 68% agreed that they knew about IS material used to create IS awareness, with 61% respondents confirming that they have firm knowledge and understanding of applicable IS policies such as MISS and ECT Act.

These results indicate that there may be bias practiced by the training unit towards certain levels or categories of employees, which could present a potential risk in that employees who have not received any training or are not given access to promotional materials on information security may be targeted by hackers and unintentionally harm the organisation, as outlined by D'Arcy et al (2007).

4.3.11 I understand the requirements and methods used for transferring, storing, labelling and handling sensitive information at the GPAA (Q16)

	Answer	Frequency	Percent	Cumulative Percent
1	Strongly agree	50	36.2	36.2
2	Somewhat agree	47	34.1	70.3
3	Neither agree nor disagree	25	18.1	88.4
4	Somewhat disagree	11	8.0	96.4
5	Strongly disagree	5	3.6	100.0
	Total	138	100.0	

Table 19 - Requirements for handling sensitive information

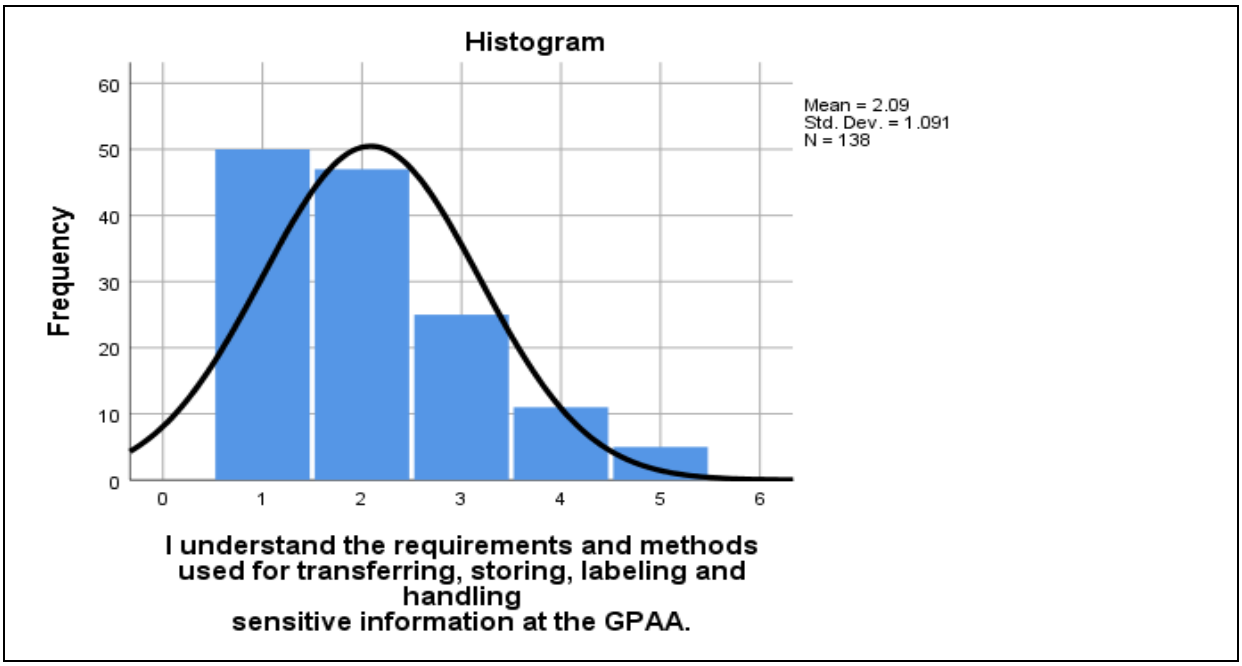


Figure 11 - Requirements for handling sensitive information

Requirements and methods used for transferring, storing, labelling and handling sensitive information are important to information security. Table 19 and Figure 11

indicate that the majority, 70.3% of the respondents agreed that they understand the requirements, methods used for transferring, storing, labelling and handling sensitive information, as it is important of information security measure, meanwhile 11.6% disagreed, and 18.1% neither agreed nor agreed. The 18.12% of participants who were neutral included 6 senior managers and this was a reflection of the low level of awareness in that group (Appendix D). 1 of the senior managers also disagreed to understanding requirements of handling sensitive information (Appendix D).Senior management play a key role in setting organisational tone, and being advocates of strategy and policies. The perceived lack of awareness by senior management on handling of sensitive information is of concern and needs to be addressed.

4.3.12 I am familiar with security programmes in place to make staff at the GPAA security conscious with regard to the protection of information security (Q17)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	49	35.5	35.5
2	Somewhat agree	47	34.1	69.6
3	Neither agree nor disagree	26	18.8	88.4
4	Somewhat disagree	14	10.1	98.6
5	Strongly disagree	2	1.4	100.0
	Total	138	100.0	

Table 20 - Familiarity with security programmes

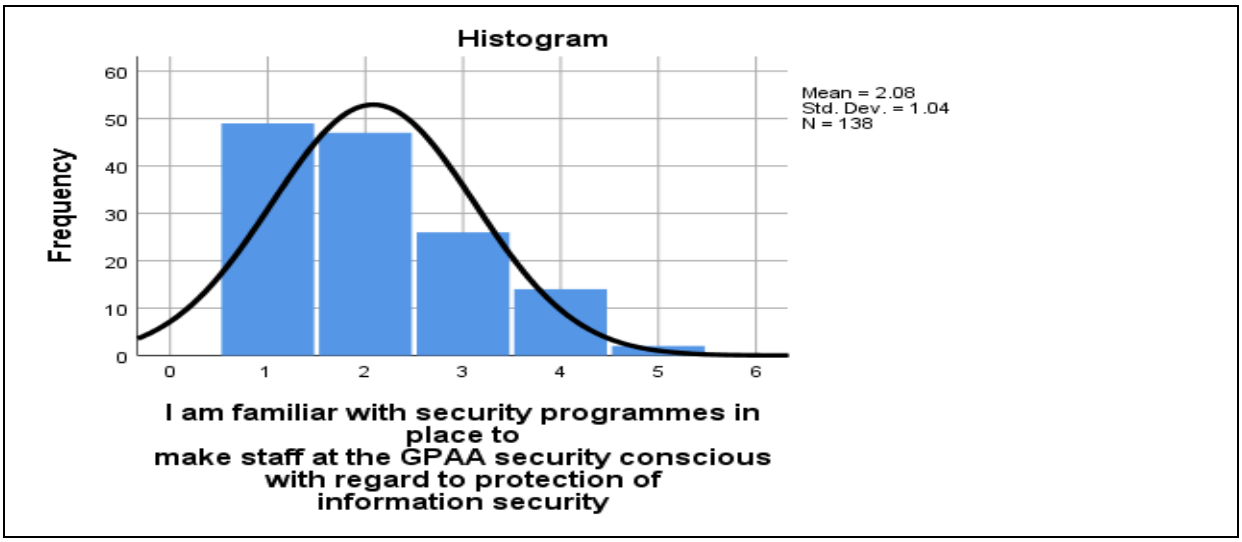


Figure 12 - Familiarity with security programmes

Security programmes highlight the importance of information security management and make the staff at the GPAA conscious of information security. Table 20 and Figure 12 reflect the views of the respondents and the majority of the respondents 69.6% agreed that they are familiar with security programmes in place. 11.5% disagreed and 18.8% neither agreed nor disagreed. Some senior managers were either neutral or disagreed with the statement, and this indicated a low level awareness even in managerial levels.

A study into the feasibility of a vocabulary test to assess information security awareness conducted by Kruger et al. (2010) specified that there is significant relationships between knowledge of concepts and behaviours of employees on Information Security. The challenge with 11.5% and the 18.8% of employees that were not in agreement with existence presents a potential problem and may affect the level of awareness on information security by GPAA employees. De Maeyer (2007) defines ISA as an ongoing and organised effort that guides the behaviour and culture of organisation on security issues. Based on De Maeyer (2007) definition, the results indicate a lack of formal programmes at GPAA, when dealing with information security related matters.

4.3.13 I do not leave sensitive data unattended in open areas (i.e. Copiers, Desks, and Faxes) (Q18)

Information security management is compromised when staff leaves sensitive information unattended. Table 21 and Figure 13 indicate the views of staff with regarding leaving sensitive information unattended.

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	86	62.3	62.3
2	Somewhat agree	31	22.5	84.8
3	Neither agree nor disagree	14	10.1	94.9
4	Somewhat disagree	4	2.9	97.8
5	Strongly disagree	3	2.2	100.0
	Total	138	100.0	

Table 21 - Leaving sensitive information unattended

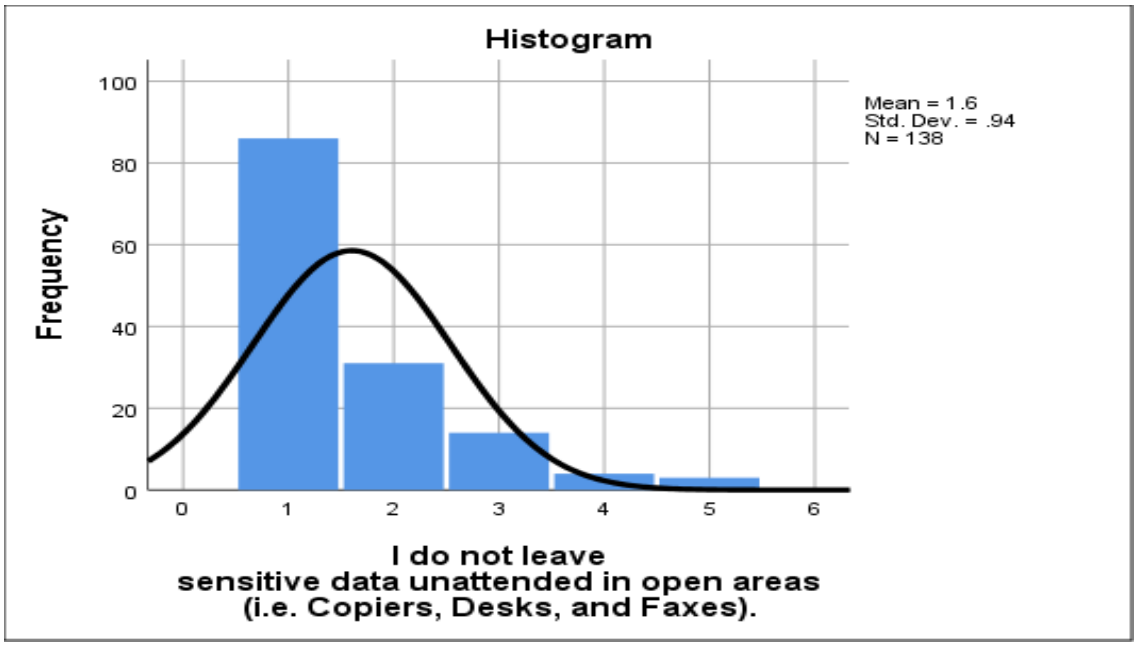


Figure 13 - Leaving sensitive information unattended

A large number, 84.8 %(Table 21) of the respondents agreed that they do not leave sensitive data unattended in open areas (i.e. Copiers, Desks, and Faxes) and 5.1% disagreed and 10.1% neither agreed nor disagreed. These results indicate that many people keep their desks clear and tidy at work, and look after their records.

4.3.14 GPAA systems do not allow unauthorised access to information of records (Q19)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	69	50.0	50.0
2	Somewhat agree	42	30.4	80.4
3	Neither agree nor disagree	16	11.6	92.0
4	Somewhat disagree	9	6.5	98.6
5	Strongly disagree	2	1.4	100.0
	Total	138	100.0	

Table 22 - Systems to manage unauthorised access

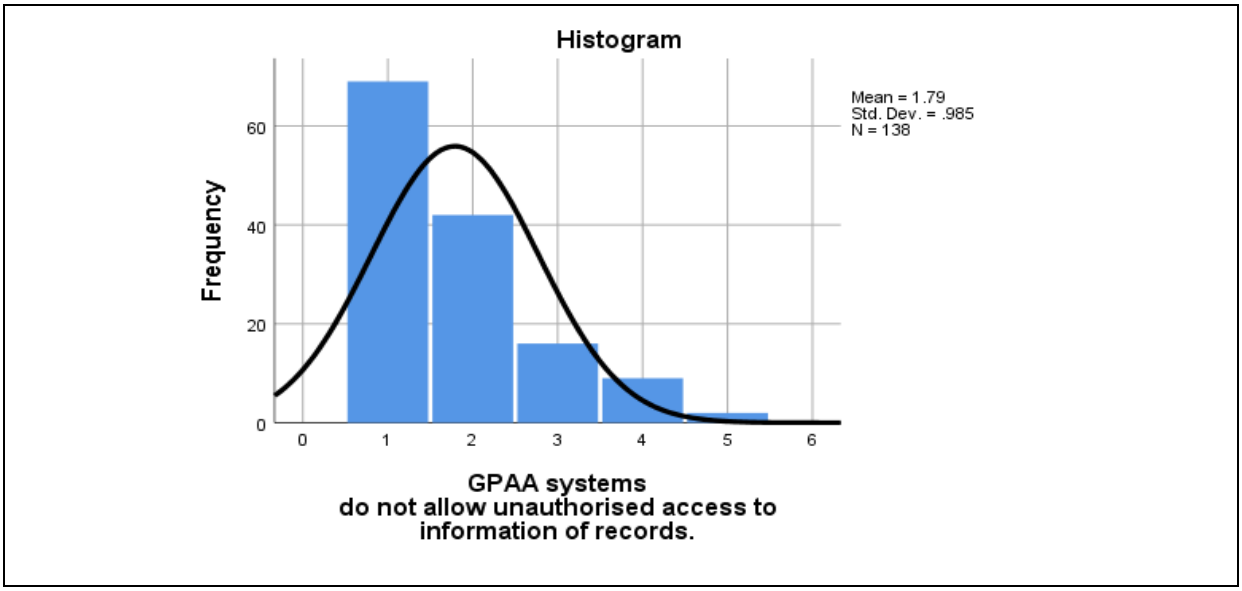


Figure 14 - Systems to manage unauthorised access

Information security depends, largely, on the systems put in place to manage access to information and records. Table 22 and Figure 14 indicate the views of employees with regard to control on systems for unauthorised access to information. A substantial number of respondents (80.4%) agreed that there are systems in place for managing unauthorised access to records of information and 8% disagreed and 11.6% neither agreed nor disagreed. This implies there a system for managing unauthorised access to information records, and employees are highly aware. A similar trend based on the previous statements was observed, where a small margin of admin and junior respondents disagreed.

4.3.15 GPAA member records can be removed without authority from their premises (Q20)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	20	14.5	14.5
2	Somewhat agree	28	20.3	34.8
3	Neither agree nor disagree	25	18.1	52.9
4	Somewhat disagree	15	10.9	63.8
5	Strongly disagree	50	36.2	100.0
	Total	138	100.0	

Table 23 - Unauthorised movement of member records

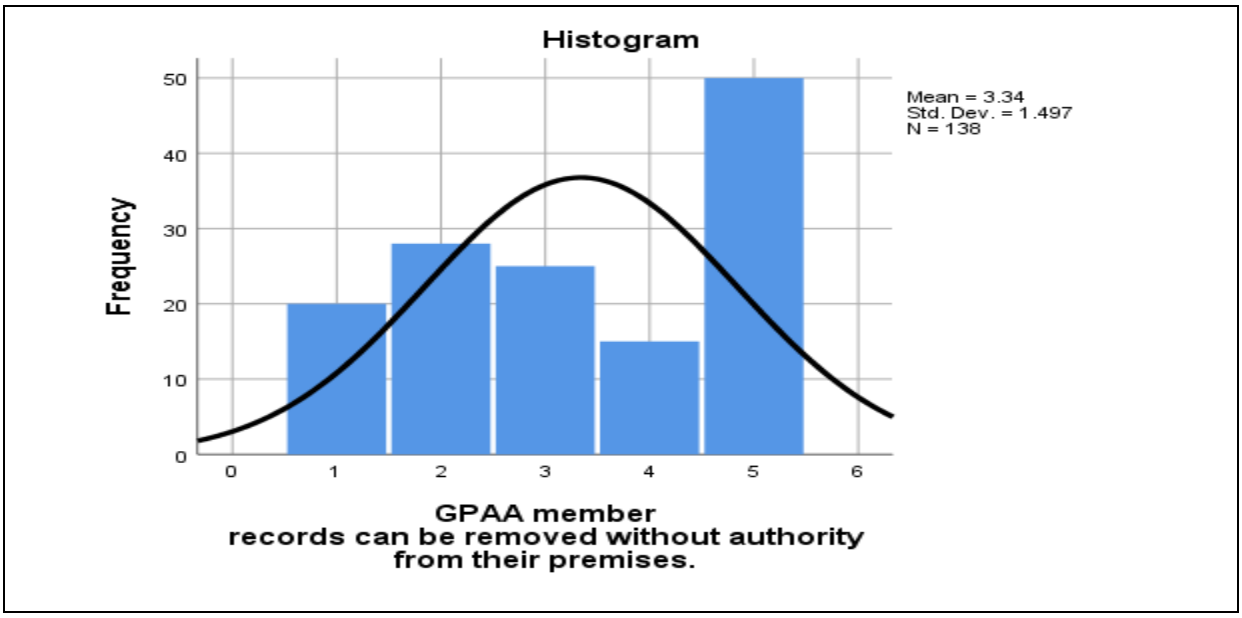


Figure 15 - Unauthorised movement of member records

The security, storage, and movement of member records are important. Records should not be moved from their premises without authority. Table 23 and Figure 15 reflect the views of the respondents as to whether member records are removed without authority from their premises. Approximately half 47.1% disagreed with the statement that "GPAA member records can be removed without authority from their premises" and just more than a quarter 34.78% agreed and 18.12% neither disagreed nor agreed. More than a quarter of the respondents, therefore, suggest that member records can be moved from their premises without authority. This is of great concern in the context that studies have shown that almost 1.4 billion worth of data was compromised in 2016 (Gemalto, 2017).

The results also indicated that there is a low level of awareness on existing security measures that GPAA has implemented, as 47.1% did not know of any security measures to protect information stored in computers. This also demonstrates ineffective security controls, and non-compliance on the MISS cabinet document. Results based on employment categories (Appendix C) and Age ranges (Appendix E) also indicates that participates from all levels and all ranges were mostly neutral in responding to the question.

According to Schwartz and Solove (2011), any organisation disseminating records of identified sensitive information must assure the reliability of the information for their intended use and must take reasonable security risk control measures to prevent the misuse of information. Files containing classified information may be easily accessed by unauthorised persons if there is no proper security risk control measure in place.

4.3.16 All employees handling sensitive information have valid security clearance certificates (Q21)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	29	21.0	21.0
2	Somewhat agree	33	23.9	44.9
3	Neither agree nor disagree	46	33.3	78.3
4	Somewhat disagree	14	10.1	88.4
5	Strongly disagree	16	11.6	100.0
	Total	138	100.0	

Table 24 - Vetting and security clearance

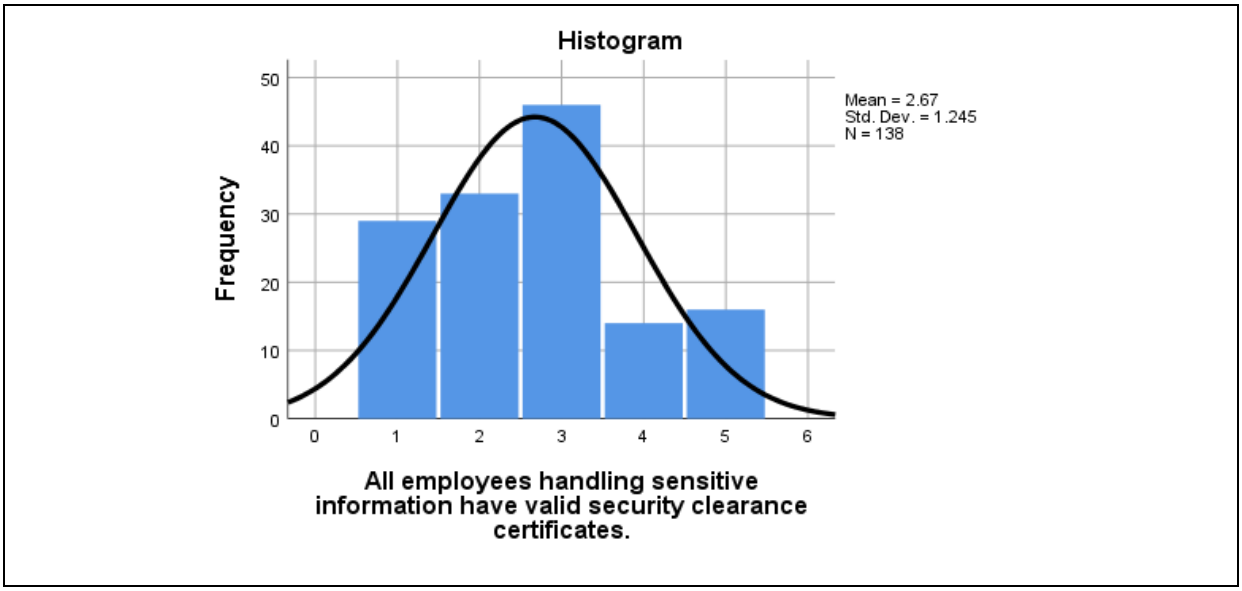


Figure 16 - Vetting & security clearance

This question was intended to test whether employees handling sensitive information have security clearance certificates. According to government policy, employees handling sensitive information should be vested and be in possession of

a security clearance certificate as a control for information security management. Table 24 and Figure 16 reflect the views of respondents on vetting and security clearance certificates. Less than half of the respondents 44.9% agreed or somewhat agreed to the statement that “All employees handling sensitive information have valid security clearance certificates” and 21.7% disagreed and 33, 3% was not sure.

There seems to be a challenge concerning vetting of officials that handle sensitive information as less than 50% indicated that it is done and a quarter of the respondents was not sure, and over 20% said it is not done. Information may be accessed by unauthorised persons. All categories of employment represent a 21.7% that disagreed with the statement. Surprisingly, the number of disagreements included senior management, who should be at the forefront of advocating and leading with information security related initiatives.

The 33.3% that was not sure also raises concern on the practice and implementation of the MISS as government policy document. With a high level of awareness as reported in question 7 that relates to familiarity of policies and responsibilities by employees, it becomes a risk to GPAA to use officials that are not vetted because classified information may be compromised (MISS reference). Documents containing sensitive information, may be leaked or shared by employees, intentionally or unintentionally which could ultimately lead to a breach of confidentiality as well as abuse of privileged information.

4.3.17 I see actions pertaining to information security as an irritant rather than assisting in securing information in the organisation (Q22)

Answer		Frequency	Percent	Cumulative Percent
1	Strongly agree	22	15.9	15.9
2	Somewhat agree	21	15.2	31.2
3	Neither agree nor disagree	39	28.3	59.4
4	Somewhat disagree	19	13.8	73.2
5	Strongly disagree	37	26.8	100.0
	Total	**138**	**100.0**	

Table 25 - The general views of employees on information security

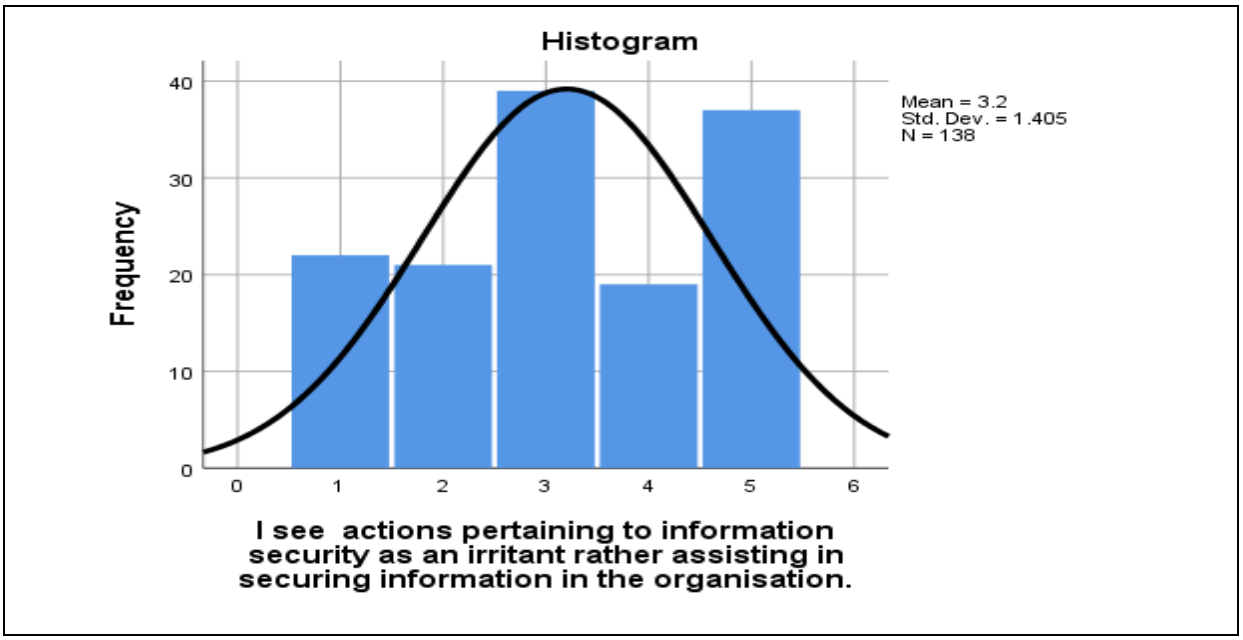


Figure 17 - The general view of employees on information security

40.6%(Table 25) of the respondents disagreed that they “see actions pertaining to information security as an irritant rather assisting in securing information in the organisation”, while a third (31.1%) agreed with the statement and 28% were not sure whether they neither agreed nor disagreed. This feedback indicates that participants should be more educated and aware of matters of information security. The different categories of employment also reflected a spread in responses, which include senior management, who agreed with the statement, therefore there is a need to increase the level of awareness and importance of information security (Appendix D).This was also the case on the different age range of employees.

5. DISCUSSIONS

5.1 The level of awareness with relevant government policy interventions, such as Minimum Information Security Standards (MISS)

Respondents believe that they are highly aware of ISPs and their responsibilities, which could be a good thing if they know what they are talking about and a very dangerous thing if they are wrong about their belief in their own knowledge. This was

demonstrated by 85.5% of responses that strongly agreed and somewhat agreed. They also understand information that is considered sensitive (89.9%) and which documents have been classified. The respondents also confirmed their knowledge in GPAA systems, i.e. it does not allow unauthorised access (80.4%), suggesting that the organisation has good information security controls. The respondents attested that there are systems and procedures to handle sensitive information and member records.

Another observation from the study on knowledge of concepts, only 61% of the respondents reported that they have a firm knowledge of legislation applicable to Information security. Of the total respondents, i.e. 138, a quarter of them (25%) neither agreed nor disagreed. This could present itself as a potential problem when dealing with information security related issued in future.

The most alarming results relate to the admin, junior and clerical staff, which scored low for information security policy and for information security programmes. The low results suggests that security policies are not well promoted or enforced by the organisation in those levels , and that emphasis maybe heavily placed on technical controls without taking into account the human aspects of information security. By not ensuring that employees become proficient in the knowledge of the organisation's policies, the policies themselves are ineffective.

The respondent's view on course materials available at the GPAA scored 68%, with other respondents, 18% who could not agree nor disagree about the availability of these materials. IS security policies need not only to be communicated to users, but also the policies should be enforced.

5.2 What is the level of awareness of the handling, transmitting and classification of records as required in the MISS Policy Document?

Most respondents had a good attitude towards information security. 63.8% agree that they know how to protect against social engineering, and 80% of the respondents attest that they know whom to contact if they suspect a security breach like phishing or virus attack. However, there are gaps in relation to the unauthorised

movement of member records from the premises. A notable concern is that only 47% disagreed with the statement, whereas more than a quarter (34%) agreed to the fact that member records can be removed from the premises. Another notable concern was that a third of the respondents see information security as an irritant rather than a control measure that needs to be embraced to protect the information the organisation. 31% agreed and 39% of respondents neither agreed nor disagreed with the statement that actions to information security are an irritant. This reflected a lack of ISA on the respondents.

The respondents generally recognise that their organisational information needs protection, and that information security was important and they should act securely in all aspects. Organisational information needs to be protected by security measures appropriate to the sensitivity of the information. The security risk control measures should protect sensitive or classified information against loss or theft, as well as unauthorised access. Employees handling sensitive information in GPAA should consider that the protection of security information is a key component of their jobs. Security breaches should be prevented at all times and Employees should ensure that such security breaches are reported.

5.3 The level of awareness with the set of controls that are currently utilised in the organization

It is of great concern that issue of vetting and clearance certificates of employees dealing with sensitive information is either not adequately done, or not done at all to some of these employees.

6. CONCLUSION

To conclude on the results of the study, the research answers the questions that were presented in sections 1.5.The sections are presented with questions and observed answers, based on the facts established during the study.

6.1 What is the general level of information security awareness at the GPAA?

An analysis of the data indicated that the participants' scores on questions relating to their knowledge were marginally higher than those testing their behaviour and attitude. The employees of the GPAA understand the importance of ISA, as 74% of them understand what constitutes an information security breach, in that they answered positively to questions relating to social engineering, phishing, and cybercrime.

Awareness programs are important educational tools in aid of preventing information security incidents and are more effective than technical security measures. The majority (69.6%) of the GPAA staff composite is aware of the security awareness programmes at the GPAA and 63.8% are cognisant with methods to safeguard against threats such as social engineering and phishing. The employees' awareness is further enforced by 68.1% of them confirming that they are aware of the course materials, security manuals and posters available on information security.

The study, therefore, confirms that the level of ISA in GPAA is perceived to be high. The information security programs and measures are however passable and need monitoring and reviewing. Achieving good ISA is imperative; unfortunately, educating users about threats, countermeasures and legislative requirements requires resources and motivation.

6.2 What is the level of information security with the set of controls that are currently utilised at the GPAA?

The employees have a commendable understanding of what constitutes "sensitive" or "classified" information (89.9%), the various classification levels of information (76.1%) and the methods and controls in place for transferring, labelling and handling sensitive information (70.3%). The data suggest that GPAA has adequate controls in place which aid with the protecting sensitive information: 84.8% of the employees indicated that they do not leave sensitive information in open unattended areas and 80.4% confirmed that GPAA systems do not grant unauthorised access to

information. The GPAA employees are currently utilising the authentication and secret knowledge measures to access and safeguard information. The majority participants (80.4%) also confirmed that they know whom to contact in the event of an information security threat.

There is, however, a concern, in that the majority of the participants neither agreed nor disagreed when asked whether sensitive information is handled by employees with valid security clearance. This suggests that although the employees know what sensitive information is, they are not certain which employees have the necessary clearance to handle the information. This aspect requires greater care and attention during awareness programs. This emphasises the notion that protecting information is dependent on the successful implementation of both information security plans and security controls.

6.3 What is the level of awareness of the relevant policy interventions such as MISS?

The responses suggest that the employees of GPAA have adequate knowledge of the applicable legislation (85.5%) and policy and/or policies (61.6%), pertaining to ISA. Compliance with these policies is not only dependant on awareness but also the perceived fairness of the information security policy, therefore ISA programs, which specifically highlight the fairness or equal application of policy is necessary.

The responses suggest that the employees of GPAA have adequate knowledge of the applicable legislation (85.5%) and policy and/or policies (61.6%), pertaining to ISA. Compliance with these policies is not only dependant on awareness alone but also the perceived fairness of the information security policy, therefore ISA programs, which specifically highlight the fairness and equal application of policy are necessary.

The participants' attitude towards information security is concerning as there was a degree of spread in the results when asked whether information security compliance amounts to an irritation rather than an assistance to the organisation. With a Mean = 3.2(Figure 17) and variance of 1.973(Table 8), the results indicate a spread in responses that Is translated in participants' different views on initiatives carried out in

educating and creating user awareness about information security. An employee's compliance with information security policies is dependent on their attitude, therefore increased attention should be given to improving the organisational attitude.

6.4 What is the level of awareness with handling, transmitting and classification of records as required by MISS?

The analysis of results suggests that the employees are aware of the minimum-security standards and measures prescribed by MISS. Their knowledge is evident in that the majority (76.1%) responded positively when posed with the question relating to the classification of sensitive information. There is a, however, a need for the GPAA to focus on the implementation of the "Information and Communication Technological Security Guidelines" and the overall aim of MISS. The need is confirmed by the participants' responses to questions relating to their awareness of course materials and security materials (68.1%), their understanding of the methods of transferring, storing, labelling and handling sensitive information (70.3%), and their familiarity of security programmes at the GPAA (69.6%).

7. RECOMMENDATIONS

7.1 General information security awareness

The literature recommends the establishment and implementation of awareness programs, as opposed to technical security measures because they are important in educating users to avoid security incidents.

It is recommended that GPAA establishes educational and training awareness programs which are aimed at educating employees and more specifically those in administrative roles on aspects such as awareness (what constitutes an information security threat) and prevention (how to prevent security incidents).

The GPAA also needs to consider hosting master classes on ISA. The audience will determine the level of complexity i.e. intermediary classes for junior managers and basic classes for the clerical and administrative staff. During these classes, the participants are educated on legislation applicable to information security, the

requirements of MISS relating to the classification of information and the storage, labelling, and handling requirements.

In order to encourage employees to participate in these awareness sessions, it is recommended that executive and senior management endorse the programs, by not only attending the training sessions but also making their staff attendance mandatory.

Yearly benchmark assessments with other institutions in government and/or surveys will aid in establishing what the employees' have knowledge of to determine if they know what they say, they know. The GPAA should, therefore, implement packaged security awareness programs, inclusive of workforce-training programs and master classes.

7.2 Vetting and security clearance

Security vetting ensures that information is protected. The GPAA should, therefore, implement pre and post-employment screening and vet all employees to strengthen the protection of information. The importance of vetting employees should also become the culture of the organisation.

8. LIMITATIONS AND FUTURE RESEARCH

8.1 Limitations

The limitation of the study is the respondents' inherent bias. The results of this report do not necessarily reflect the participants' attitude and behaviour as they are based on a self-report, therefore some respondents may be influenced by their bias. Respondents may intentionally or unintentionally adapt their responses to ensure that they are represented in a positive light. Previous research does, however, suggest that the measurement of subjective elements such as an individual's perceptions, attitudes, and knowledge is possible via self-report. The survey was conducted anonymously to decrease the influence of bias, and to increase the chance of obtaining open and honest responses. The use of internet data collection

also contributed to the limitation, as the survey was only accessed by internet uses results in limited responses, and only accessed by internet users.

8.2 Future studies

The first step is to assess the level of ISA within the organisation, the next step is to determine what methods or best practices may be implemented to resolve the problem areas identified in this study. Future research should be focused on the development and improvement of the GPAA's levels of information security awareness, therefore incorporating ISA as an integral part of organisation security strategy, to ensure that the organisation is protected against the risks and threats associated with information security breaches.

REFERENCES

Africa, S. (1996). *Constitution of the Republic of South Africa, 1996 - Chapter 10: Public Administration*. Cape Town: National Legislative Bodies / National Authorities Retrieved from https://www.gov.za/documents/constitution-republic-south-africa-1996-chapter-10-public-administration.

Africa, S. (1998). *Minimum Information Security Standards*. Retrieved from http://www.right2info.org/resources/publications.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al-Awadi, M., & Renaud, K. (2007). *Success factors in information security implementation in organizations.* Paper presented at the IADIS International Conference e-Society.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Aytes, K., & Conolly, T. (2003). A research model for investigating human behavior related to computer security. *AMCIS 2003 Proceedings*, 260.

Babbie, E. R. (2013). *The basics of social research*: Cengage Learning.

Bayat, M., & Fox, W. (2007). A guide to managing research. *Cape Town: Juta*.

Boyce, J., & Jennings, D. (2002). *Information assurance: managing organizational IT security risks*: Butterworth-Heinemann,London.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *AMCIS 2009 Proceedings*, 419.

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

Burnett, M., & Kleiman, D. (2006). Perfect Passwords: Selection. *Protection, Authentication, Syngress, Waltham, MA*, 28.

Butler, R., & Butler, M. (2014). *An assessment of the human factors affecting the password performance of South African online consumers.* Paper presented at the HAISA.

Chen, H., & Li, W. (2014). *Understanding Organization Employee's Information Security Omission Behavior: an Integrated Model of Social norm and Deterrence.* Paper presented at the PACIS.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

De Maeyer, D. (2007). Setting up an effective information security awareness programme. In *ISSE/SECURE 2007 Securing Electronic Business Processes* (pp. 49-58): Springer.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers & Security, 26*(1), 36-43.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley, Reading, MA, 1975.

Galvez, S. M., & Guzman, I. R. (2009). Identifying factors that influence corporate information security behavior. *AMCIS 2009 Proceedings*, 765.

GPAA. (2015). *Government Pension Administration Agency ICT Vulnerability Management Monitoring 2015 Current State Assessment Report*. Ernst and Young.

Gross, J. B., & Rosson, M. B. (2007). *End user concern about security and privacy threats.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.

ISO. (2005). Information Technology: Security Techniques: Code of Practice for Information Security Management. ISO/IEC.

Istitute, P. (2017). 2017 Cost of Data Breach Study: Global

Overview. from IBM securityhttps://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/security-ibm-security-services-se-research-report-sel03130wwen-20180122.pdf

Johnson, E. C. (2006). Security awareness: switch to a better programme. *Network security, 2006*(2), 15-18.

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*(5), 316-327.

Laaksonen, E., & Niemimaa, M. (2011). Information Security Policies: A Frames of Reference Perspective. In.

Leedy, P., & Ormrod, J. (2010). Practical Research Planning and Design. New Jersey, US: Pearson Education. In: Inc.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622-660.

Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Morgan, R., & Boardman, R. (2012). *Data protection strategy: implementing data protection compliance* (Vol. 8): Sweet & Maxwell.

Ngoepe, M. S. (2008). *An exploration of records management trends in the South African public sector: a case study of the Department of Provincial and Local Government.*

Pretorius, B., & Van Niekerk, B. (2015). *Cyber-security and governance for ICS/SCADA in South Africa.* Paper presented at the Proceedings of the 10th International Conference on Cyber Warfare and Security.

Qing, T., Ng, B.-Y., & Kankanhalli, A. (2007). Individual's Response to Security Messages: A Decision-Making Perspective. In *Decision Support for Global Enterprises* (pp. 177-191): Springer.

Qudaih, H. A., Bawazir, M. A., Usman, S. H., & Ibrahim, J. (2014). *Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization*.

Rogers, E. M. (2003). Elements of diffusion. *Diffusion of innovations, 5*(1.38).

Rogers, F. (2005). Security practice III/Security Risk Management IV: SEP361/SRM4015. In: Florida: Technikon SA.

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev., 86*, 1814.

Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Computers and Society, 31*(2), 24-29.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Stephanou, A. (2009). *The impact of information security awareness training on information security behaviour.*

Struwig, M., Struwig, F., & Stead, G. (2001). *Planning, reporting & designing research*: Pearson South Africa.

Sukamolson, S. (2007). Fundamentals of quantitative research. *Language Institute Chulalongkorn University*, 1-20.

Thomson, M. (1999). *Making information security awareness and training more effective.* Paper presented at the Proceedings of the IFIP TC11 WG11.

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security, 2006*(6), 17-19.

Van Der Westhuizen, A., Schellnack-kelly, I., & Geyer, R. (2010). *Basic Archives adn Records management course*. Pretoria: UNISA Centre for Applied Communication.

Van Niekerk, J. F. (2005). *Establishing an information security culture in organizations: An Outcomes Based Education Approach.* Nelson Mandela Metropolitan University Port Elizabeth,

Von Solms, B. (2006). Information security–the fourth wave. *Computers & Security, 25*(3), 165-168.

Von Solms, R., Thomson, K.-L., & Maninjwa, M. (2011). *Information security governance control through comprehensive policy architectures.* Paper presented at the Information Security South Africa (ISSA), 2011.

Vroom, C., & von Solms, R. (2002). A practical approach to information security awareness in the organization. In *Security in the Information Society* (pp. 19-37): Springer.

Wagner, A. E., & Brooke, C. (2007). Wasting Time: The Mission Impossible with Respect to Technology-Oriented Security Approaches. *Electronic Journal of Business Research Methods, 5*(2).

Welman, J., Kruger, S., & Mitchell, B. (2005). Research Methodology. Cape Town: Oxford University Press Southern Africa.

APPENDIX A – Information Security Survey

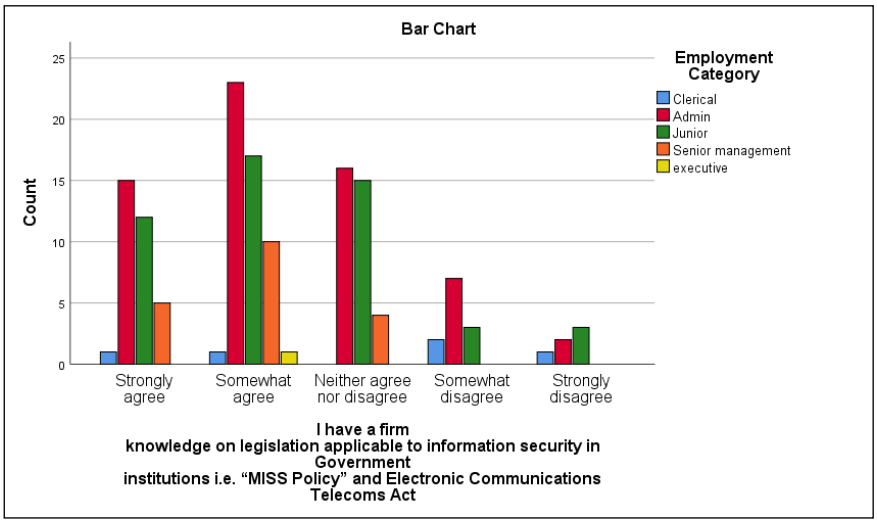
APPENDIX B – Approval to conduct research

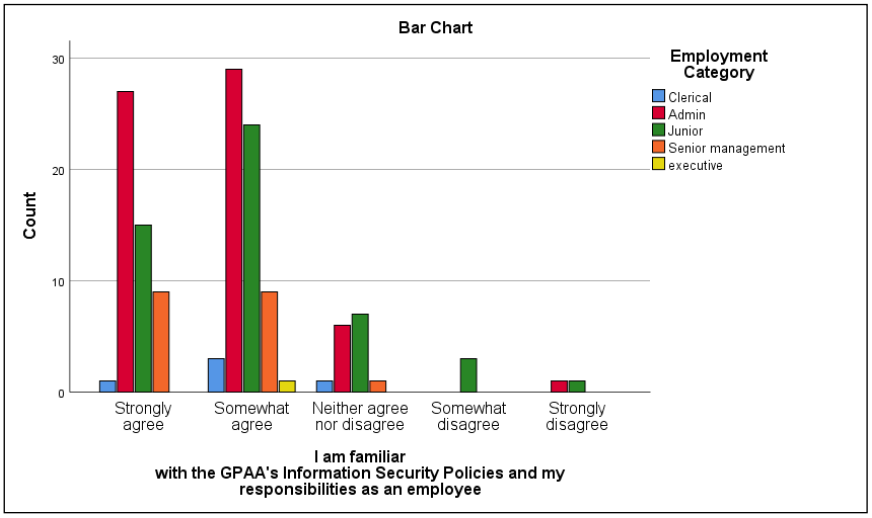
APPENDIX C - Group Statistics: comparison of Means - gender

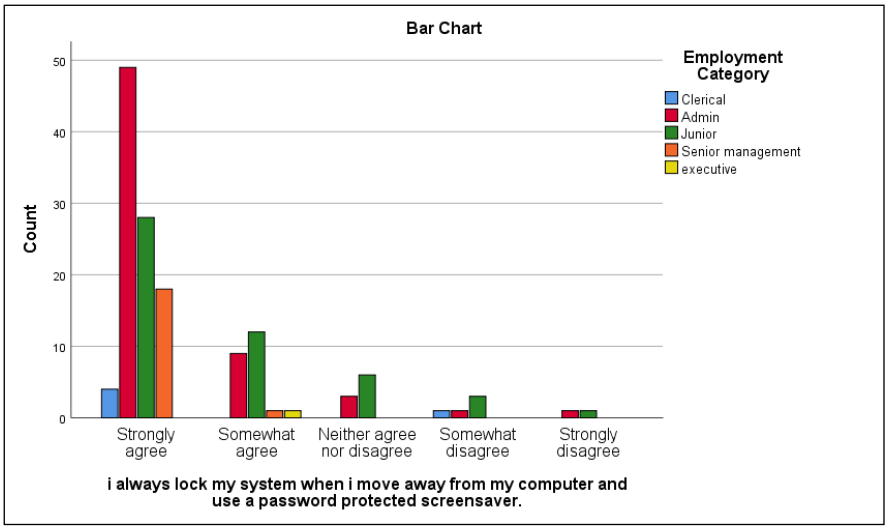
Survey Questions	Gender	N	Mean	Std. Deviation	Std. Error Mean
I have a firm knowledge of legislation applicable to information security in Government institutions i.e. “MISS Policy” ECT Act	Male	55	2.13	1.001	.135
	Female	83	2.45	1.096	.120
I am familiar with the GPAA's Information Security Policies and my responsibilities as an employee	Male	55	1.85	.931	.126
	Female	83	1.80	.745	.082
I always lock my system when I move away from my computer and use a password protected screensaver	Male	55	1.62	1.045	.141
	Female	83	1.36	.742	.081
I understand the requirements for and use of strong passwords	Male	55	1.35	.775	.105
	Female	83	1.20	.488	.054
I know and understand the term " social engineering" Phishing" and " Cyber Crime"	Male	55	2.02	1.114	.150
	Female	83	2.05	1.125	.124
I know how to protect against “social engineering”,” phishing” and “cybercrime”	Male	55	2.13	1.139	.154
	Female	83	2.47	1.151	.126
I know when and who to contact if I am suspicious of any information security incident/threat.	Male	55	1.87	1.037	.140
	Female	83	1.83	.960	.105
I understand what information is considered “sensitive” or “classified” at the GPAA	Male	55	1.53	.900	.121
	Female	83	1.58	.798	.088
Documents containing sensitive information are classified according to their levels of classification (Restricted, Confidential, and Top Secret) at the GPAA.	Male	55	1.89	1.083	.146
	Female	83	1.90	1.055	.116
I am aware of course materials, security manuals and	Male	55	2.18	1.249	.168

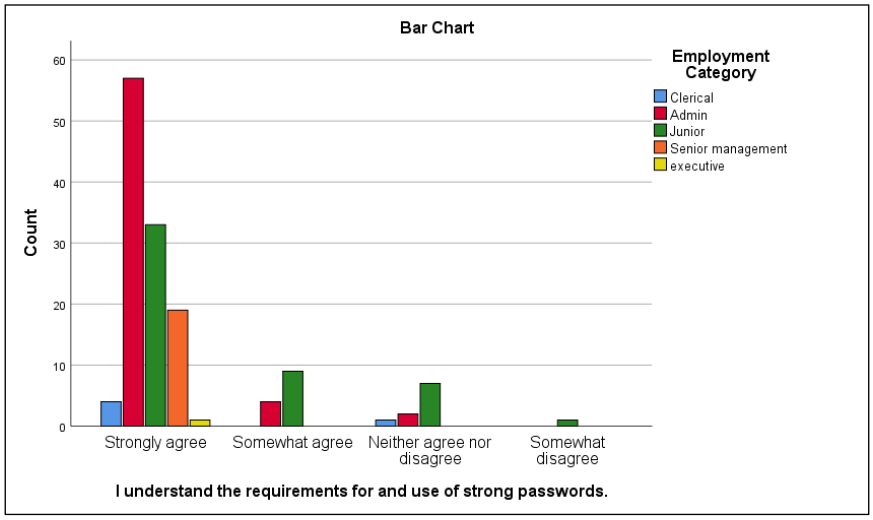
Survey Questions	Gender	N	Mean	Std. Deviation	Std. Error Mean
posters on information security, available at the GPAA, and know how to access them.	Female	83	2.14	1.026	.113
I understand the requirements and methods used for transferring, storing, labelling and handling sensitive information at the GPAA.	Male	55	2.16	1.167	.157
	Female	83	2.04	1.041	.114
I am familiar with security programmes in place to make staff at the GPAA security conscious with regard to the protection of information security	Male	55	2.16	1.118	.151
	Female	83	2.02	.987	.108
I do not leave sensitive data unattended in open areas (i.e. Copiers, Desks, and Faxes).	Male	55	1.69	.979	.132
	Female	83	1.54	.915	.100
GPAA systems do not allow unauthorised access to information of records.	Male	55	1.78	.994	.134
	Female	83	1.80	.985	.108
GPAA member records can be removed without authority from their premises.	Male	55	3.22	1.512	.204
	Female	83	3.42	1.491	.164
All employees handling sensitive information have valid security clearance certificates.	Male	55	2.80	1.325	.179
	Female	83	2.59	1.190	.131
I see actions pertaining to information security as an irritant rather assisting in securing information in the organisation.	Male	55	3.24	1.478	.199
	Female	83	3.18	1.363	.150

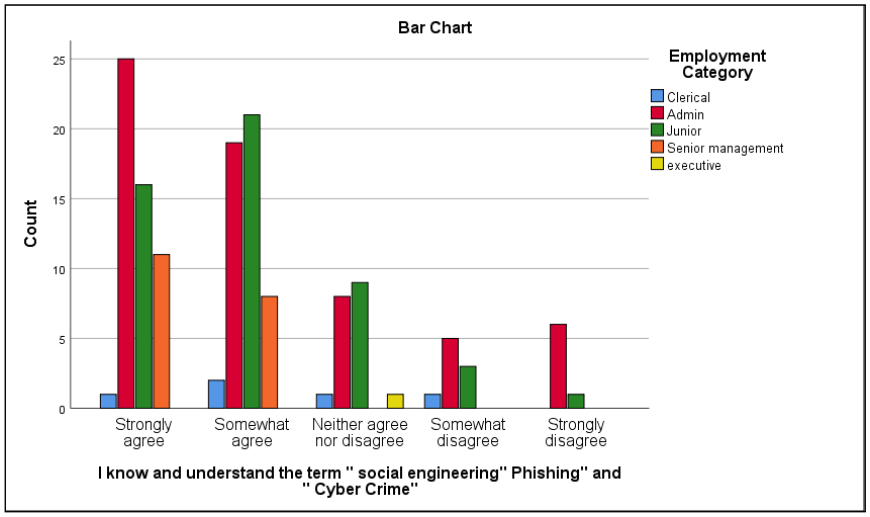
APPENDIX D – Descriptive statistics: employment category

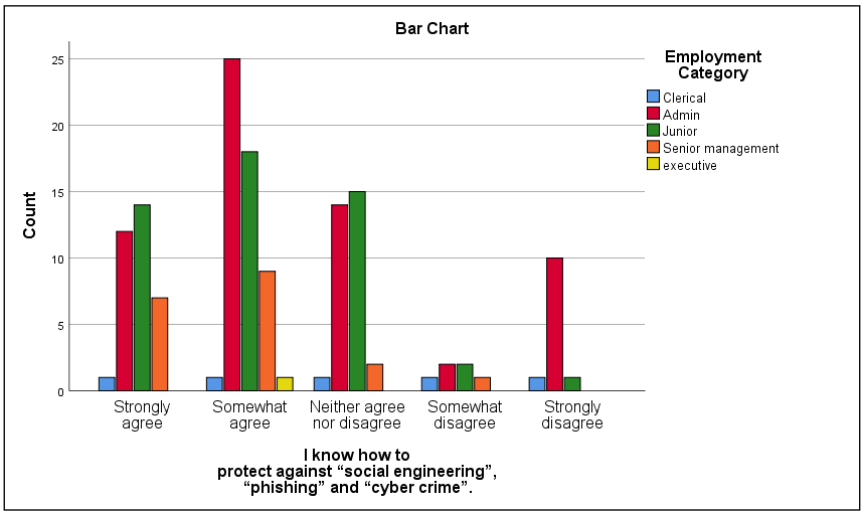


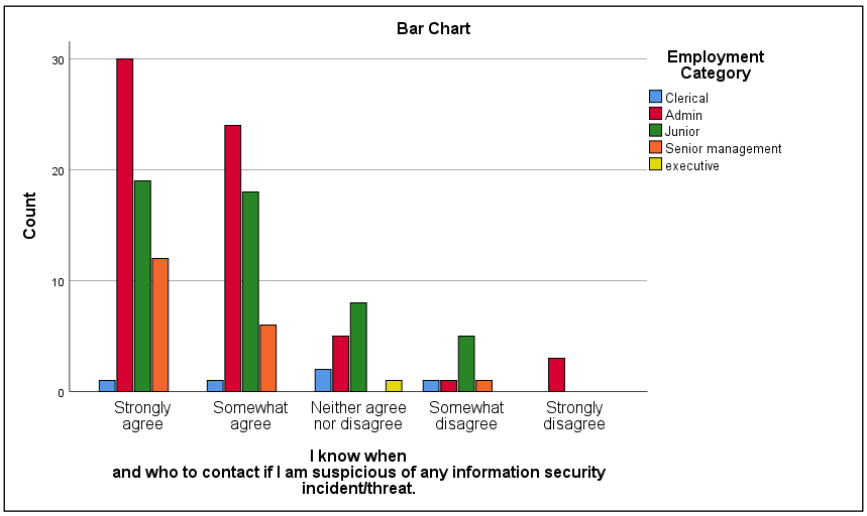


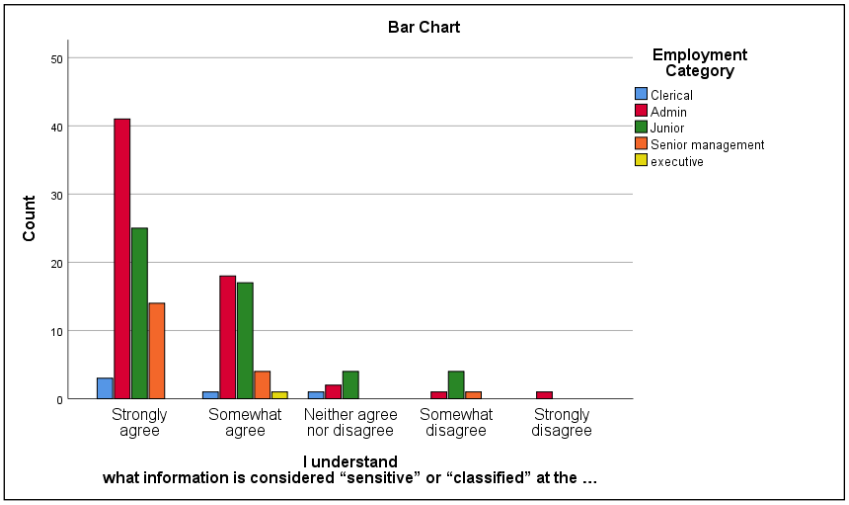


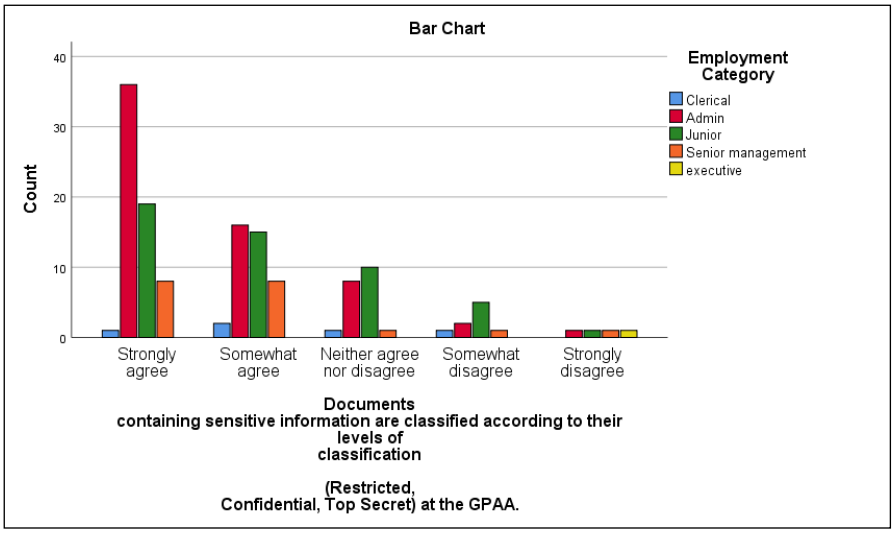

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
60
50
40
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
I understand the requirements for and use of strong passwords.

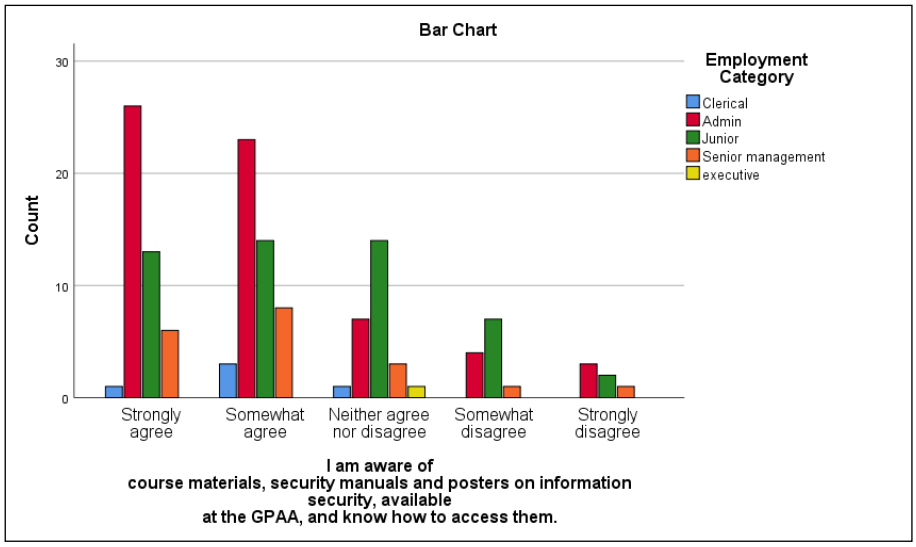

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
25
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I know and understand the term " social engineering" Phishing" and " Cyber Crime"

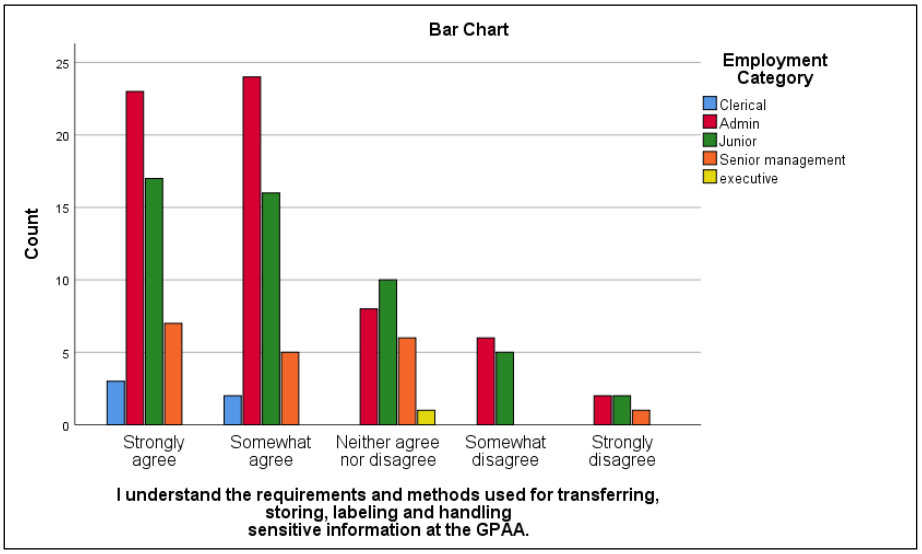

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
25
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I know how to protect against "social engineering", "phishing" and "cyber crime".

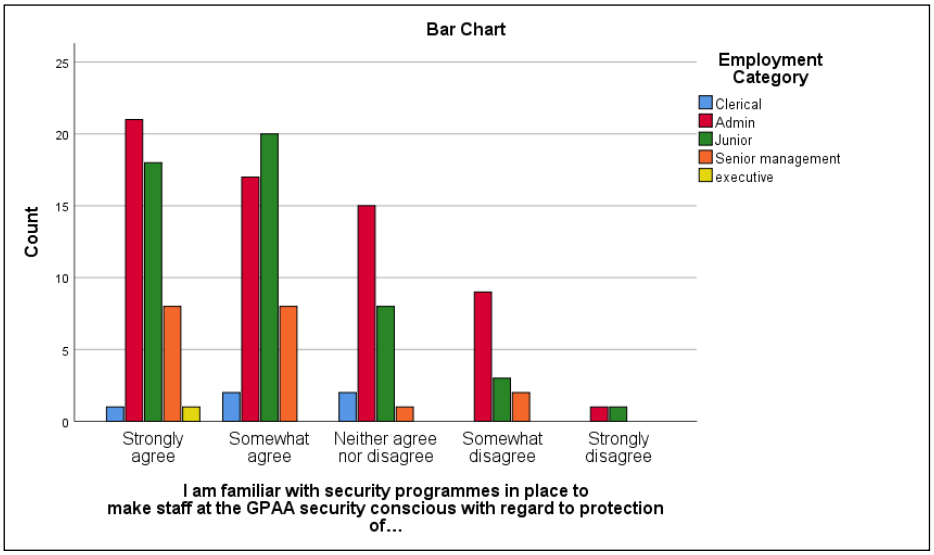

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I know when and who to contact if I am suspicious of any information security incident/threat.

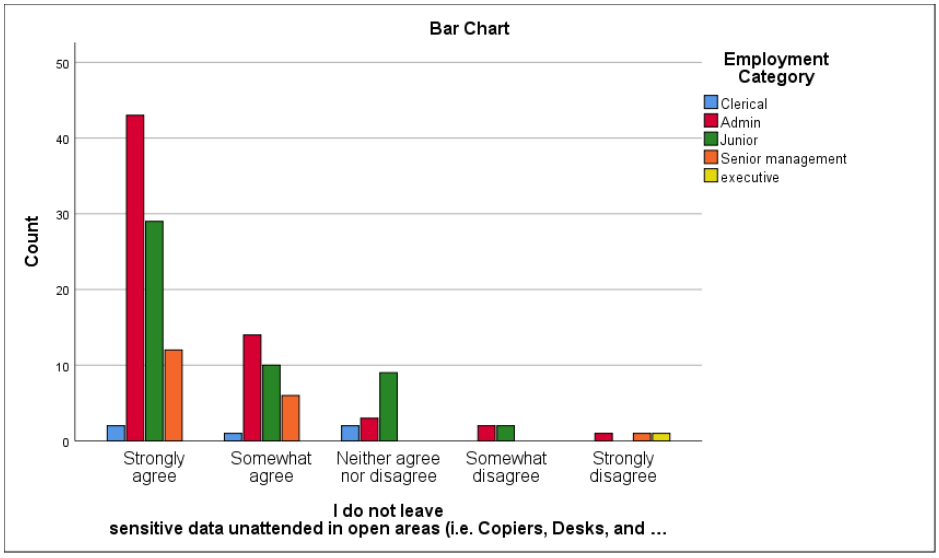

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
50
40
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I understand what information is considered “sensitive” or “classified” at the …

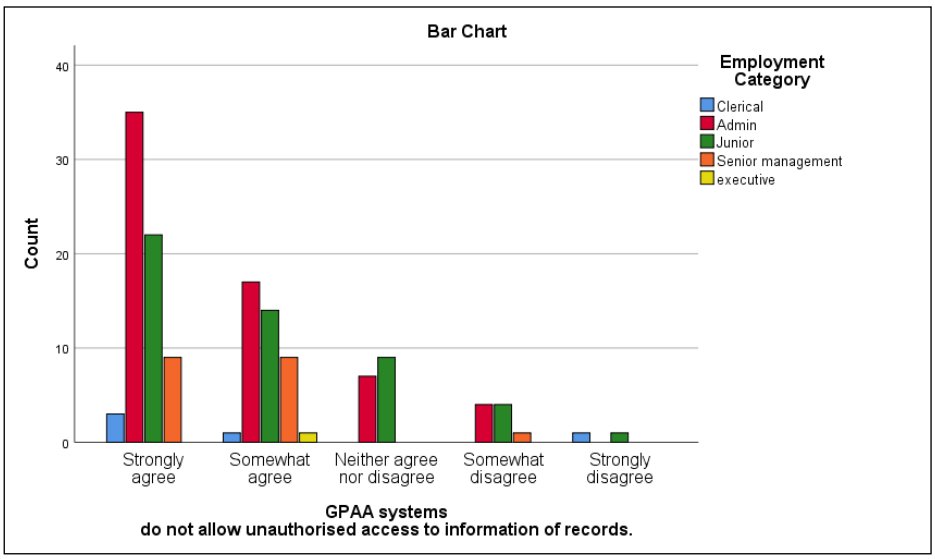

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
40
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
Documents containing sensitive information are classified according to their levels of classification (Restricted, Confidential, Top Secret) at the GPAA.

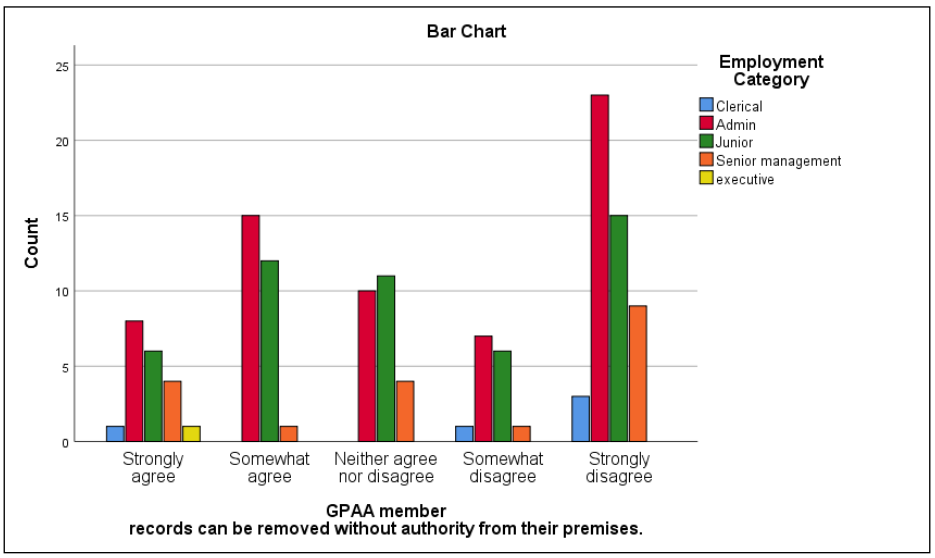

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I am aware of course materials, security manuals and posters on information security, available at the GPAA, and know how to access them.

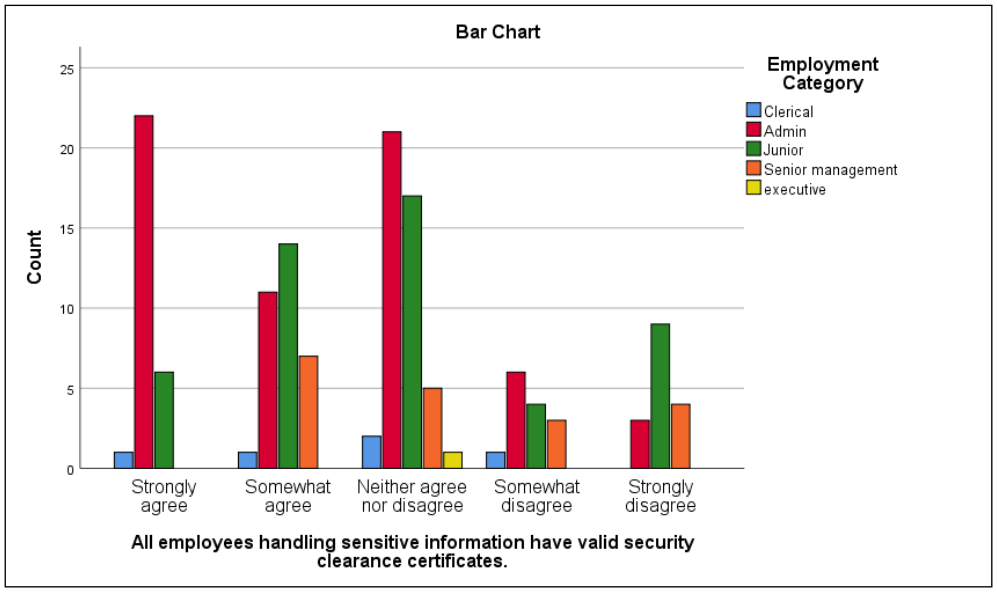

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
25
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I understand the requirements and methods used for transferring, storing, labeling and handling sensitive information at the GPAA.

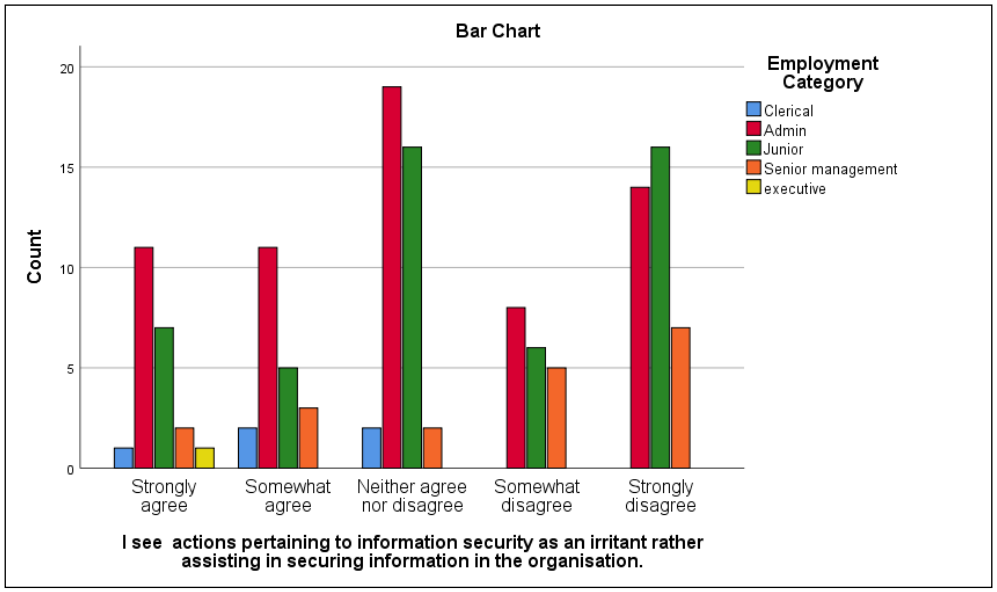

Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
25
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I am familiar with security programmes in place to make staff at the GPAA security conscious with regard to protection of…


Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
50
40
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I do not leave
sensitive data unattended in open areas (i.e. Copiers, Desks, and ...


Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
40
30
20
10
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
GPAA systems
do not allow unauthorised access to information of records.


Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
25
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
GPAA member
records can be removed without authority from their premises.


Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
25
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
All employees handling sensitive information have valid security clearance certificates.


Bar Chart
Employment Category
Clerical
Admin
Junior
Senior management
executive
Count
20
15
10
5
0
Strongly agree
Somewhat agree
Neither agree nor disagree
Somewhat disagree
Strongly disagree
I see actions pertaining to information security as an irritant rather assisting in securing information in the organisation.

APPENDIX E: Group Statistics – comparison of Means Age Range

Survey questions	Age Range	N	Mean	Std. Deviation
Q6 – knowledge of ISA concepts	15 – 25	3	2.67	1.528
	26 – 35	43	2.40	1.050
	36 – 45	51	2.35	1.128
	45 and above	41	2.17	.998
Q7 – familiarity with ISA and own responsibilities	15 – 25	3	2.00	1.000
	26 – 35	43	1.88	.793
	36 – 45	51	1.96	.958
	45 and above	41	1.56	.594
Q8 – use of passwords and screen saver	15 – 25	3	2.67	1.528
	26 – 35	43	1.56	.934
	36 – 45	51	1.45	.856
	45 and above	41	1.29	.750
Q9 – Use of strong passwords	15 – 25	3	2.00	1.000
	26 – 35	43	1.23	.571
	36 – 45	51	1.25	.659
	45 and above	41	1.24	.582
Q10 – knowledge & understanding of terms	15 – 25	3	2.67	1.155
	26 – 35	43	1.86	1.082
	36 – 45	51	2.16	1.138

Survey questions	Age Range	N	Mean	Std. Deviation
	45 and above	41	2.02	1.129
Q11 - How to protect against IS threats	15 – 25	3	2.00	.000
	26 - 35	43	2.19	1.118
	36 - 45	51	2.41	1.203
	45 and above	41	2.41	1.183
Q12 – Knowledge of who to contact	15 - 25	3	1.33	.577
	26 - 35	43	1.84	.949
	36 – 45	51	1.98	1.049
	45 and above	41	1.73	.975
Q13 – Knowledge of sensitive and classified data	15 - 25	3	1.33	.577
	26 - 35	43	1.65	.897
	36 - 45	51	1.69	.927
	45 and above	41	1.32	.610
Q14 – Classification of records	15 - 25	3	1.33	.577
	26 - 35	43	1.77	.895
	36 - 45	51	2.04	1.166
	45 and above	41	1.90	1.114
Q15 – Awareness of information security material	15 - 25	3	1.33	.577
	26 - 35	43	2.07	1.142
	36 - 45	51	2.39	1.218

Survey questions	Age Range	N	Mean	Std. Deviation
	45 and above	41	2.02	.935
Q16 – Requirements for handling sensitive information	15 - 25	3	1.67	1.155
	26 - 35	43	1.81	1.006
	36 - 45	51	2.31	1.225
	45 and above	41	2.12	.954
Q17 – Familiarity of security programmes	15 - 25	3	1.33	.577
	26 - 35	43	2.16	1.111
	36 - 45	51	2.24	1.050
	45 and above	41	1.85	.937
Q18 – leaving sensitive information unattended	15 - 25	3	1.33	.577
	26 - 35	43	1.53	.909
	36 - 45	51	1.73	.981
	45 and above	41	1.54	.951
Q19 – Systems to manage unauthorised access	15 - 25	3	1.33	.577
	26 - 35	43	1.81	.932
	36 - 45	51	1.75	.977
	45 and above	41	1.85	1.085
Q20 – Unauthorised movement of records	15 - 25	3	3.67	1.528
	26 - 35	43	3.19	1.435
	36 - 45	51	3.24	1.582
	45 and above	41	3.61	1.464
Q21 – Vetting and security clearance	15 - 25	3	2.00	.000

Survey questions	Age Range	N	Mean	Std. Deviation
	26 - 35	43	2.60	1.256
	36 - 45	51	2.49	1.271
	45 and above	41	3.02	1.193
Q22 – General views of employee information security	15 - 25	3	3.00	1.000
	26 - 35	43	2.98	1.371
	36 - 45	51	3.16	1.461
	45 and above	41	3.51	1.381