THE ROLE OF VULNERABILITY DISCLOSURE PROGRAMS IN AN ORGANISATIONAL CYBERSECURITY STRATEGY

By

Trishee Jobraj

Student Number: 200100522

A dissertation submitted in partial fulfilment of the requirements for the degree of

Master of Commerce Coursework in Information Systems and Technology

College of Law and Management Studies

School of Management, Information Technology and Governance

SUPERVISOR: Karunagaran Naidoo

2020

DECLARATION

I, Trishee Jobraj, declare that:

i. The research reported in this dissertation/thesis, except where otherwise indicated, is my original research.

ii. This dissertation/thesis has not been submitted for any degree or examination at any other university.

iii. This dissertation/thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

iv. This dissertation/thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a) their words have been re-written but the general information attributed to them has been referenced;

   b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. Where I have reproduced a publication of which I am author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

vi. This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signed: ……. Date: …….

DEDICATION

This research is dedicated to my daughter. One day you will be a wife, mother, employee, friend, sibling and a student. That's when life will really test you. But no matter what obstacles life throws at you, never give in to them, keep your chin up and always strive to complete what you have started. It may not be easy, but it is possible.

Always remember "If you can see the invisible, you can achieve the impossible." Shiv Khera

ACKNOWLEDGEMENTS

I wish to start off by thanking God for always guiding me and giving me the strength to see it to completion. It has been a long journey!

I would like to express my gratitude to my family for their love, support and encouragement throughout my long academic journey.

- To my parents for always pushing me to learn and grow.
- To my husband for his love, support and assisting me along the way.
- To my brother for always being there for me.

I wish to express my sincere appreciation to the following individuals whose help made this research possible:

- My supervisor, Mr. Karunagaran Naidoo for his guidance, advice and for always understanding and supporting me through my personal situations during this journey.
- My boss, Mr. Junaid Amra for understanding & supporting my personal goals.
- Mr. Barend. H. Pretorius for assisting with my statistics and advising me on my research.
- Mr. Justin. J. Williams for always encouraging me and supporting the topic.
- My Colleagues and Friends for the daily words of encouragement and support.
- All the participants that took the time to complete my questionnaire.

LIST OF ACRONYMS AND ABBREVIATIONS

CEO	Chief Executive Officer
CAE	Chief Audit Executive
CIO	Chief Information Officer
CIS	Centre for Internet Security
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
COJ	City of Johannesburg
CVE	Common Vulnerabilities and Exposures
IODSA	The Institute of Directors in Southern Africa
IOL	Independent Online
IOT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardisation
IT	Information Technology
NIST	National Institute of Standards and Technology
PWC	PricewaterhouseCoopers
SA	South Africa
SABRIC	South African Banking Risk Information Centre
SMB	Server Message Block
TAM	Theory Acceptance Model (TAM)
TPB	Theory of planned behaviour
US CERT	United States Computer Emergency Readiness Team
UTAUT	Unified Theory of Acceptance
VDP	Vulnerability Disclosure Program
ZDI	Zero Day Initiative

ABSTRACT

Today's world is a technological one, with devices and software becoming more interconnected. Inherent to these devices and software are vulnerabilities that if discovered by malicious parties, may be exploited. In order to discover, investigate and remediate these vulnerabilities timeously with little or no impact to users, organisations have started to invest in vulnerability disclosure programs (VDP). This provided researchers with a platform in order to communicate discovered vulnerabilities to the organisation in a standardised and consistent manner. It also provided organisations with a method of detecting security flaws that were not normally detected by vulnerability scanners. VDP's assist in identifying these vulnerabilities in a coordinated manner to facilitate speedy remediation.

This research investigated the challenges and benefits of VDP's and the need for such a program as part of the organisational cybersecurity strategy.

Quantitative analysis was used to conduct the study by means of an online questionnaire. 147 participants who were members of ISACA South Africa spread across South Africa, with Information Technology (IT) and cybersecurity experience, responded to the questionnaire. The questionnaire measured the opinions, views and experience of the various stakeholders. The questionnaire comprised of rating and ranking scales such as the Likert scale in order to obtain a rich and accurate data set for analysis. The questionnaire data was analysed using descriptive analysis (i.e.: frequency analysis, mean and standard deviation) and correlation. Statistical analysis tools such as PSPP and Real Statistics which is an add on in Excel were used to analyse the data. Based on the research performed, the key findings were around the lack of awareness of VDP's in the IT and cybersecurity space within South Africa. This included the understanding of the types of VDP's as well as the processes associated with VDP's as well as the lack of management support towards VDP's. It was also evident that many organisations did not have an official channel to report VDP's.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Background

Technology and software are in continual use in our daily lives from devices such as smartphones, computers, to our home appliances and cars (Pupillo, 2017). Each of these technologies and software that assist us to be interconnected is also at risk of security vulnerabilities. These vulnerabilities can be exploited by threats in order to cause service disruption or comprise the products quality and operability.

Vulnerbilities are on the increase. In 2018, approximately 16,555 Common Vulnerabilities and Exposures (CVE's) were listed, indicating that there would be no decreasing in 2019 (Sass, 2019). This was possibly due to a few reasons such as more code being developed by inexperienced people, hence it was deemed not as secure (Sass, 2019). Security and quality was not high on the priority list as getting the product out quickly to customers was key (Gayomali, 2014). There was also an increase in devices known as the Internet of Things (IOT) devices from wearables such as smart watches to smart home devices such as smart televisions and refrigerators, with applications developed to interface with them (Sass, 2019). These devices result in an increase in the vulnerability exposure.

The 2018 bug bounty report published by Bugcrowd highlighted that there was an increase in the number of cybersecurity vulnerabilities that were exploited in the past year. (Bugcrowd, 2018). Cybersecurity is the process of securing systems, networks, and software from cyberattacks. These cyberattacks were usually aimed at obtaining access to or modifying sensitive information, stealing or extorting money from user, or disrupting business operations (Cisco, 2019). The goal of cybersecurity was to maintain the confidentiality, integrity and availability of information and information resources. Organisations were adopting VDP's in order to improve their cybersecurity posture (US DOJ, 2017). It was therefore important for organisations to have a method to communicate discovered vulnerabilities.

By including a VDP as part of the cybersecurity strategy, organisations would ensure that vulnerabilities were detected and mitigated in a coordinated and timeous manner. This research focused on the challenges and benefits of VDP's and the need for such a program as part of the organisational cybersecurity strategy.

1.2 Motivation for Study

There have been numerous occurrences across the world of people being arrested for identifying and attempting to disclose security vulnerabilities in organisation's publicly accessible systems (Williams, 2016). Some of these organisations interpreted these disclosures as negative publicity. However, there were some organisations that encouraged this type of engagement to assist in securing their systems by remediating vulnerabilities timeously (Williams, 2016).

The bug bounty report published by Bugcrowd highlighted that there was an increase in the number of cybersecurity vulnerabilities that were exploited in the past year (Bugcrowd, 2018). These included vulnerabilities such as Wannacry, Petya, NotPetya, Meltdown and Spectre. The Wannacry ransomware was a worm that exploited the Microsoft server message block (SMB) 1.0 vulnerabilities in Windows operating systems, across the world in 2017. The ransomware infected machines and encrypted the files so that they would not be accessible until a ransom was paid. Wannacry affected numerous computers over 150 countries, including South Africa (Rouse, 2018). Petya and NotPetya were malware that encrypted the computer hard drive and demanded a ransom. The malware spread world-wide by exploiting the same SMB vulnerability as Wannacry (Fruhlinger, 2017). Meltdown and Spectre exploited vulnerabilities in processors which allowed malicious programs to steal sensitive data (Graz University of Technology, 2018). These vulnerabilities could have been detected earlier with the implementation of the appropriate remediation to protect the affected systems (Ruohonen & Allodi, 2018). VDP's could have been used to discover some of these vulnerabilities to alert the affected organisations (National Cyber Security Centre, 2018).

In order to stay ahead of cyber threats, organisations started to invest in a VDP, as an early warning system, that detected and disclosed security flaws that were not normally detected by vulnerability scanners.

1.3 Research Problem

The interconnectedness of technology and systems brought with it an increase in vulnerabilities. These vulnerabilities could be exploited by malicious parties as part of cybercrime or disruption of service (National Telecommunications and Information Administration, 2015). Vulnerability disclosure programs (VDP) assisted in identifying these vulnerabilities in a coordinated manner to facilitate speedy remediation. However, there was limited research around on the challenges and benefits of VDP's and whether it should be included in the overall cybersecurity strategy.

Vulnerability disclosure programs played an important role in identifying the security flaws that were not usually detected by vulnerability scanners. This research focused on the challenges and benefits of VDP's and the need for such a program as part of the organisational cybersecurity strategy.

1.4 Justification for the Study

There was limited information available on the challenges and benefits of implementing VDP's and whether it should be implemented as part of a cybersecurity strategy. This study assessed the challenges and benefits of VDP's within a South African context and the need for such a program as part of a cybersecurity strategy. There was also limited information available on the implementation of VDP's within South Africa, therefore this study will fill this knowledge gap.

1.5 Research Aim and Objectives

The aim of this research was to explore the challenges and benefits of VDP's and the need for such a program as part of the organisational cybersecurity strategy.

This research will satisfy the following research objectives:

- To determine the challenges associated with vulnerability disclosure programs.
- To determine the benefits associated with vulnerability disclosure programs.
- To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy.

1.6 Research Questions

This research answered the following research questions:

- What are the challenges associated with vulnerability disclosure programs?
- What are the benefits associated with vulnerability disclosure programs?
- Should a vulnerability disclosure program be implemented as part of an overall cybersecurity strategy?

1.7 Significance of the Study

This study provided a South African context to VDP's. VDP's within South Africa was still in its infancy stage and have not yet been fully implemented. There were limited studies done in South Africa on this topic and this research contributed to the body of knowledge.

1.8 Research Methodology

This section outlines the research methodology used in the study and covers the research design, approach, study site and sampling strategy.

1.8.1 Research Design

According to Bhattacherjee (2012) an exploratory research was conducted when a study had not been done in a specific area. This was done to investigate the scope, obtain preliminary designs and to determine whether there was opportunity to perform further study on the phenomenon. The main goal of this study was to obtain an understanding of the benefits and challenges of VDP's and the need for such a program as part of the organisational cybersecurity strategy. Therefore, an exploratory design methodology was suitable to conduct this study as it created new knowledge and served as a precursor for further research. The scope of this research was limited to South Africa, and therefore may not have general applicability.

1.8.2 Research Approach

Qualitative analysis focuses on the study of the core or underlying aspects such as feelings and reasons (Bhattacherjee, 2012). The gathering, analysis and reporting of numerical data is defined as quantitative analysis. Quantitative analysis was selected to conduct the study by means of an online questionnaire as it focused on known facts that were based on predictable outcomes. The questionnaire comprised of various rating and ranking scales such as the Likert scale to obtain a rich and accurate data set for analysis. The questionnaire was distributed electronically via email and social media platforms by the South African chapter of the international organisation Information Systems and Audit Control Association (ISACA) to their member base.

1.8.3 Study Site

The research was based in South Africa with Information Technology (IT) and cybersecurity professionals that was affiliated with the South African chapter of the international organisation Information Systems and

Audit Control Association (ISACA). The research questionnaire was distributed by ISACA South Africa via email and social media platforms to their members.

1.8.4 Sampling strategy

This research used non-probability convenience sampling of the IT and cybersecurity professionals that are affiliated with the South African chapter of the international organisation Information Systems and Audit Control Association (ISACA). Convenience sampling as stated by Kothari (2004), is performed when objects in the target population are selected because of ease of access. The sample used in this research was chosen from IT and cybersecurity professionals that have the knowledge of and experience with vulnerability disclosure programs. According to the sample table recommended by Sekaran & Bougie (2010), the sample size for the questionnaires that was recommended to be used in this study, was 329 respondents across ISACA South Africa at a 95% confidence level and 5% marginal error rate. However, due to the poor response rate, only 147 responses were received. According to an email delivery report received from ISACA SA, of the 2326 emails that were sent out only 765 emails were opened. This was 33% of the population. ISACA SA continued to share the survey with their members on a weekly basis, via email and their social media platforms, however, limited responses were received. As a result, the target population used in this study was the 765 opened emails as it provided some assurance in terms of email delivery. This had a sample size of 256, which represented a 57% response rate in terms of the sample size. Additionally, according to (Sekaran & Bougie, 2013), a response rate of 30% is acceptable. Furthermore, the data collected represented 9 provinces, 13 industries and 12 different job functions across South Africa. As a result, the 147 responses were deemed suitable for this study as it provided insight into the state of VDP's within South Africa.

1.9 Data collection method

In order to the conduct this study, a research questionnaire was circulated to the target population. Bhattacherjee (2012) stated that a questionnaire was a type of research instrument that consisted of questions that was intended to obtain the responses from participants in the study in a structured manner. This instrument was suitable for quantitative analysis using the statistical analysis tools. The questionnaire used closed questions and comprised of various rating and ranking scales such as the Likert scale in order to obtain a rich and accurate data set for analysis. The data that was gathered through the research questionnaires, was examined using descriptive analysis (i.e.: frequency analysis, mean and standard deviation) and correlation. Singh (2006) stated that descriptive analysis was concerned with the facts and could be used over a national geographic spread at minimal costs and effort. The researcher had prior knowledge and understanding of the statistical analysis tools PSPP and Real Statistics which was an add on in Excel. As a result, these tools were used to analyse the data.

1.10 Ethical Consideration

The researcher submitted a research proposal on the topic to the Higher Degrees Committee of the School of Management, Information Technology and Governance at University of KwaZulu-Natal. Once the research proposal was approved, a gatekeeper's letter was requested from the ISACA South Africa Chapter in order to distribute the questionnaire to their members. Refer to Appendix 2 for the gate keeper's letter. The researcher then requested ethical clearance from the University of KwaZulu-Natal Research Office. Comments on the ethical clearance application were addressed by the researcher and resubmitted for approval. Thereafter, ethical clearance was obtained. Refer to Appendix 3 for the ethical clearance approval letter. In terms of ethical consideration, prior to participation in the survey, informed consent, that was on a separate document and based on adequate knowledge of the study, was requested from all participants. Personal information was not required on the questionnaire. The confidentiality and anonymity of the participants was ensured.

1.11 Limitations of the study

The questionnaire was only sent out to the ISACA South Africa community to understand their responses. There may have been a limitation with the sampling methods selected, as other respondents outside ISACA South Africa could have responded but were not fully identified. Another limitation is that the respondents may have ignored or forgotten about the questionnaire that was emailed to them through ISACA South Africa.

1.12 Structure of the research

The study was documented in chapters. These were arranged as Chapter 1 to Chapter 5 of the study and are outlined below:

- **Chapter 1:** This is an introductory chapter that provides an overview of the study. It describes the motivation for the research, problem statement, objectives and research questions. It also highlights the research methodology to be used in the study as well as the significance and limitations.

- **Chapter 2:** This chapter provides an overview of existing literature relating to vulnerabilities, vulnerability disclosure programs and frameworks from a South African and Global perspective. This forms the theoretical basis for the study.

- **Chapter 3:** This chapter outlines the research methodology that was used for the study. The reasons for choosing the quantitative approach, the sampling strategies, the data collections methods and ethical considerations are described.

- **Chapter 4:** In this chapter the data collected and analysed during the study is presented and discussed. The results of the analysis have been interpreted in terms of the research objectives.

- **Chapter 5:** This is the concluding chapter of the research and highlights the findings and limitations of the research as well as recommendations for further research.

1.13 Conclusion

This chapter provided an outline of the background and significance of the study regarding vulnerability disclosure programs. It has introduced the research problem, objectives and questions that was the focus of the study. The research methods and analysis methods required for the study has been described along with the limitations of the study. The following chapter provides an overview of existing literature relating to vulnerabilities, vulnerability disclosure programs and frameworks from a South African and Global perspective. This forms the theoretical basis for the study.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This is a literature review chapter and focuses on what vulnerabilities and VDP's were, the types of VDP's, why VDP's were important and the challenges and benefits of VDP's. It also touches on what cybersecurity is, cybersecurity statistics in South Africa, as well as frameworks that supported VDP's.

2.2 What is a vulnerability?

Errors could occur in the process of designing and developing a software or technology. These were known as vulnerabilities (Rapid7, 2019). A vulnerability, in information technology (IT), was an error in the code or design that created a possible point of compromise for a device, system or network (TechTarget, 2019). Vulnerabilities provided an avenue that an intruder could use to access a system or force a software to behave in a different manner. Vulnerability detection could occur during the requirement gathering and analysis, design, implementation or coding, testing, deployment or maintenance phase of the product development lifecycle; however, many vulnerabilities were only detected after the system or software was implemented in the production environment (Wysopal, 2002). Traditional vulnerability assessments were performed by one or two resources following a standard approach and methodology with vulnerability scanners. Given the large number of vulnerabilities, it was not possible for this approach to detect all high-risk vulnerabilities and to have them remediated timeously. VDP's play a role in vulnerability detection in the production environment as it utilised human intelligence to identify vulnerabilities (Bugcrowd, 2018). VDP's created a relationship of cooperation between security researchers and organisations.

2.3 What are vulnerability disclosure programs and why are they important?

The practice of reporting security flaws in computer software and/ or hardware was known as vulnerability disclosure (Searchsecurity, 2019). These were reported by security researchers directly to the affected organisation or publicly for them to be fixed timeously.

A VDP offered a secure method for security researchers to report and disclose security vulnerabilities which included processes for responding to and remediating the identified vulnerabilities (Porup, 2018). This provided good-faith security researchers a platform to communicate discovered vulnerabilities and help the industry. According to Wysopal (2002), the goal of VDP's included the following:

- Ensuring that vulnerabilities could be identified and remediated appropriately for all parties.
- Minimising the risk to customers systems cause by vulnerabilities.
- Providing customer with enough information to understand and evaluate the security levels in products.
- Providing security researchers with enough and appropriate information to assist in the development of methods and tools for the identrification, management and reduction of vulnerabilities.
- Minimising the time spent by resources to manage vulnerabilities.
- Facilitating research and development of tools and process that could assist with the management and remediation of vulnerabilities.

Once a vulnerability was discovered, the following steps were executed by the security research community (Searchsecurity, 2019).

- Vulnerability discovery, understanding its impact and documenting the location of the vulnerability through screenshots or code.
- Creating an advisory report that contained details and evidence of the vulnerability a full disclosure timeline which was submitted to the vendor.

- The vendor was given a period to investigate and remediate the discovered vulnerability in accordance with the disclosure timeline.
- If a patch was made available by the vendor or if the disclosure timeline has elapsed, the researcher publicly published a full disclosure analysis of the exploit which included details of the vulnerability, its impact and resolution.

The steps taken by the security research community was dependent on their motivation. This ranged from recognition in the form of online credits, name on the hall of fame, swag, ensuring the products that they use were secure or monetary rewards (Pubal, 2017).

The study by Algarni & Malaiya (2013) on the motivation and methods of vulnerability researchers, highlighted that researchers were motivated by various factors such as hobby and lifestyle, curiosity, enjoyment, profit and auditing. Some of the motivation could have been malicious but a lot of the research was performed with the motive of detecting a vulnerability and communicating it to the affected individual or organisation (Pubal, 2017). “Providing rewards to motivate people to find software defects or weaknesses before they are exploited by black hat exploiters is critical to improving computer security.” (Algarni & Malaiya, 2013, p. 3).

2.4 Types of vulnerability disclosure programs

There were a few categories that described the way a vulnerability was disclosed. Many confuse VDP’s with bug bounties, but they are vastly different (Porup, 2018).

2.4.2 Descriptions of vulnerability disclosure programs

Table 1 below describes the different types of vulnerability disclosure programs with examples of organisations that have implemented them.

Vulnerability Disclosure Type	Description	Source	Examples
Non-disclosure	A vulnerability was discovered by a researcher and kept a secret. This was often practiced by black-hat hackers.	(Cencini, Yu, & Chan , 2005)	None
Self-disclosure	Vendors learned about the flaws themselves and then published them whilst publishing patches or other remediation steps.	(Searchsecurity, 2019)	Trend Micro Zero Day Initiative (ZDI)
Responsible-disclosure	The parties that report the vulnerabilities did not own the system. These were done by security researchers who notify the vendors directly or via a coordinating third party in order work to develop fixes for the vulnerability.	(Searchsecurity, 2019)	MTN South Africa Nike JPMorgan Chase Standard Bank Barril Group Bidorbuy MultiChoice Mimecast
Full-disclosure	All details of the vulnerability were released in public, sometimes as soon as the	(Pupillo, 2017)	Openbugbounty Hackerone Bugcrowd

Vulnerability Disclosure Type	Description	Source	Examples
	information of the vulnerability were identified and often without resolutions.		
Bug Bounties	Incentivised security researchers to disclose vulnerability discoveries. The aim was to have the vendor remediate the vulnerability before the public was made aware of it.	(NTIA, 2015)	Apple Microsoft Yahoo Facebook Google Dropbox Intel

Table 1. Types of VDP's

(Source: Researcher compiled)

Table 1 highlights the few instances where organisations have implemented VDP's. According to a vulnerability research report conducted by Frost & Sullivan, self-detected vulnerabilities or vulnerabilities detected by security researchers were disclosed to the public for Core Security, FortiGuard Labs, Google Project Zero, Secunia Research, US CERT, and Trend Micro Zero Day Initiative (ZDI) (Frost & Sullivan, 2018). The report also noted that only 2% of the reported vulnerabilities were self-disclosed. This highlighted the low implementation rate of VDP processes and the understanding thereof within these organisations.

It was noted that VDP's created a level of responsibility and transparency for individual organisations affected by vulnerabilities, web hosting service providers and software providers who may not have been

writing secure code and practicing due diligence (Frost & Sullivan, 2018). Furthermore, it assisted in creating a standardized approach on how vulnerabilities are tracked, managed and stored.

2.4.2 Organisational examples of vulnerability disclosure programs

MTN South Africa and Standard bank made use of a managed platform through Hackerone. Hackerone stated that their platform was the industry standard for security that was based on hacker research. They partnered with the global hacker research community to bring to light the most relevant security issues for their customers before they could be exploited (Hackerone, 2019). This platform created a base for researchers and white hat hackers to identify vulnerabilities and disclose them in a coordinated manner and had the following benefits:

- ISO compliant defined processes;
- A community of researcher and hackers;
- Validation of vulnerabilities; and
- Processing of payments should there be rewards offered.

Another managed platform, similar to Hackerone, was Bugcrowd. Bugcrowd offered VDP and Bug Bounty Programs that could meet crowdsourced security needs. These executed together could maximise the scale of ingenuity and exposure that could not be matched by other vulnerability assessment tools or services (Bugcrowd, 2018). These types of platforms created an ideal way for organisations that did not have the skills or resources to create an internal VDP.

An analysis of the website of South African company Barril Group, indicated that the company implemented a responsible disclosure program. Their aim was to keep their websites, online services and applications safe for their customers. They expressed that security of data was important to them (Barril Group, 2019). The policy and process to be followed was defined and articulated on the web page with clear

indication that monetary rewards would not be offered. Barril Group also welcomed the white hat security researchers and listed the activities that these researchers were not permitted to perform.

A review of the website for South African company Bidorbuy, highlighted that a responsible disclosure program was implemented. It was stated that the company valued the work of security researchers in order to improve their products and services. They further stated that they were committed to working with the research community to confirm, replicate and respond to valid disclosed vulnerabilities. They encouraged the research community to participate in their VDP (Bidorbuy, 2016). The company mentioned that in order to encourage responsible disclosure that they would not take legal action against reporters of vulnerabilities, if the responsible disclosure guidelines were complied with.

MultiChoice in South Africa implemented a responsible disclosure program. Their aim was to keep their services secure for their customers with security of data being most important (MultiChoice, 2019). The website stated the policy and process for reporting vulnerabilities and made no mention of rewards for verified security vulnerabilities. International company Mimecast had a responsible disclosure website that included the policy and process for reporting vulnerabilities and a security research wall of fame for verified vulnerabilities, dating back to 2015 (Mimecast, 2019).

A review of international company, Nike's VDP showed that a responsible disclosure program had been implemented which provided a clear process for communicating vulnerabilities. The website stated that it was not a bug bounty program and that no compensation or reward was provided for detected vulnerabilities. It also stated what information was required in order to remediate a vulnerability and how Nike would respond (Nike, 2019).

A review of the website for International company JPMorgan Chase & Co, identified that a responsible disclosure program was implemented. The policy for disclosure, type of vulnerabilities that would be

accepted were documented. There was no mention of rewards or recognition for accepted vulnerabilities. (JPMorgan Chase & Co, 2019)

Studies showed that VDP's that used bug bounties could assist in the detection of website vulnerabilities such as cross site scripting (Ruohonen & Allodi, 2018). A review of Intel's VDP, highlighted the implementation of a bug bounty program. Intel incentivised security researchers to disclose security vulnerabilities (Intel, 2019). The process was clearly articulated with conditions for reporting and how the rewards and recognitions were determined. The more difficult a vulnerability was to remediate; the more Intel would pay.

Based on google scholar searches and searches on the University of Kwa-Zulu Natal's online library on VDP implementations, supported by the reviews mentioned above, highlighted that very few South African companies have implemented vulnerability disclosure programs. Most of the websites of companies only included an email address for reporting any vulnerabilities and did not include a disclosure policy and/ or process. These websites also did not mention rewards or recognitions. There were also limited studies on the challenges and benefits of VDP's.

2.5 Challenges and Benefits

The NTIA vulnerability disclosure report that spread across 50 countries, such as the United Kingdom, United States of America, Australia and India, revealed that " 60% of the respondents feared they may be subject to legal proceeding if they disclose their work" and that less than 1 in 5 companies made use of VDP's such as bug bounties. 54% highlighted that VDP's reduced marketing and development costs (National Telecommunications and Information Administration, 2015, p. 6).

The disclosure of some vulnerabilities may have assisted in the improvement of the organisations/ vendors cybersecurity posture, however, in many instances there were associated costs that outweighed the benefits. These included the exploitation of vulnerabilities by black-hat hackers, financial costs to investigate the incidents, fix vulnerabilities, create and distribute patches (Cencini, Yu, & Chan , 2005).

The article by Vidstrom (2002) showed that vulnerability disclosures assisted in driving developers to create patches faster in order to prevent exploitation and protect the users. This further assisted in updating vulnerability scanners so that penetration testers had the latest vulnerabilities. The article also stated that disclosing vulnerabilities created the risk that exploits could occur before a fix was made available.

Organisations were noted to take too long to remediate vulnerabilities resulting in exposure to potential data breaches. Certain industries such as the financial and education could take up to 176 days to fix (Barker, 2015). According to the 2017 global public vulnerability research report, VDP's assisted in demonstrating the importance of detecting and remediating detected vulnerabilities (Frost & Sullivan, 2018). The 2018 bug bounty report stated that "Services such as bug bounty and vulnerability disclosure programs leverage human intelligence at scale to deliver rapid discovery of high-risk vulnerabilities across attack surfaces." (Bugcrowd, 2018, p. 17).

The information above suggests that there were pro's and con's associated with VDP's. This research will delve deeper into the challenges and benefits of VDP's and it's role in implementing VDP's as part of a cybersecurity strategy.

2.6 Cybercrime statistics

The PwC 22nd Annual Global CEO Survey that was conducted across 91 territories globally such as the United States, China, Germany, United Kingdom and Australia, indicated that CEO's have ranked cyber

threats as the fifth threat that they were extremely concerned about. In South Africa, 38% of the surveyed CEO's were extremely concerned about cyber threats (PwC, 2019). The South African Banking Risk Information Centre (SABRIC) reported that in South Africa, victims of cyber-crime lost approximately R2.2 billion a year because of cyber-attacks (IOL, 2018). As part of the South African Edition of the Global Economic Crime and Fraud Survey for 2018, 28% of the respondents felt that cyber-crime would be the most disruptive crime to be experienced over the next 2 years, thus requiring enhanced due diligence (PwC, 2018). The article by Symantec on cybersecurity predictions for 2019, highlighted that the cybersecurity risks associated with cybercrime, cyber espionage, cyber warfare and hacktivism would increase in 2019 (Thompson & Trilling, 2018).

In South Africa, the City of Johannesburg (COJ) website had a vulnerability that was discovered by a user in 2013. He disclosed the discovery on an internet forum stating that it exposed customer information from statement to account numbers and pin. He was discredited by COJ as a hacker with malicious intent (BusinessTech, 2013).

The information highlighted by these cyber incidents emphasised the need for VDP's in order to provide a platform that could detect and disclose vulnerabilities in a secure and efficient manner. VDP's would have provided the means and processes to assist in the disclosure and remediation of a vulnerability (Hackerone, 2019). In order for VDP's to get the appropriate level of attention for proper implementation, it needs to be considered as part of cybersecurity program or strategy (Ben-Avie, 2017).

2.7 What is cybersecurity?

Cybersecurity is the process of securing systems, networks, and software from cyberattacks. These cyberattacks were usually aimed at obtaining access to or modifying sensitive information, stealing or extorting money from users, disrupting business operations (Cisco, 2019). The International Organisation

for Standardisation (ISO) stated that the primary concern of cybersecurity was the "confidentiality, integrity and availability of information" (International Organization for Standardisation, 2013). In today's interconnected world, cybersecurity plays an important role, as the risk of cyber threats are actively increasing. VDP's should be part of the overall cybersecurity strategy with policies, frameworks and/ practices that govern the overall management. These are discussed further below.

2.8 Cybersecurity laws, Standards, Governance frameworks and Regulations

Online searches on Google Scholar as well as the online library at the University of Kwa-Zulu Natal resulted in the identification of cybersecurity laws, standards, governance frameworks and regulations that contained controls related to vulnerabilities and vulnerability disclosure. These highlighted how VDP's fit into a cybersecurity strategy and are presented below.

2.8.1 King IV

The King IV code was developed by The Institute of Directors in Southern Africa (IODSA) for good corporate governance. Principle 12 of The King IV code stated that the governing body should oversee technology and information in a manner that supports the organisation in achieving its strategic objectives (KPMG South Africa, 2016). This framework supported the creation of VDP's as part of an organisational strategy.

2.8.2 CIS Controls

The Centre for Intermet Security is a non-profit organisation that developed cybersecurity controls and benchmarks that assists in safeguarding organisations against cyber threats (Cisecurity, 2019). Control 19 of the CIS Controls V7 stated that an organisations information, reputation should be protected by the development and implementation of an incident response infrastructure. This includes plans, roles and responsibilties, training and communications and management oversight. This would assist in the quick discovering of an attack, containment of damage, removing the attacker and restoring systems and network (Cisecurity, 2019). This control supported the creation of VDP's as part of a cybersecurity strategy.

2.8.3 NIST Special Publications 800-53 (Rev.4)

The National Institute of Standards and Technology (NIST) is physical science laboratory in the United States Department of Commerce (NIST, 2017). NIST developed the NIST Special Publications 800-53 (Rev.4) to assist with cybersecurity. Control AC-21 on Information Sharing from the NIST Special Publication 800-53 (Rev. 4) stated that information systems enforced information-sharing based decisions by authorised users that were based on access authorisations of the sharing partners and the access restrictions on the information to was to be shared (NVD, 2019). This highlighted that organisations could share vulnerability information if it was implemented in accordance with the organisations policies and standards in terms of access restrictions and data classification.

2.8.4 ISO/IEC 29147:2018

The International Organisation for Standardisation (ISO) is an organisation that develops standards that assist organisations in fields of technical activity (ISO, 2018). ISO/IEC 29147:2018 provided guidance on the disclosure of identified vulnerabilities in products and services. It outlined the process a vendor could use to address vulnerability related issues (ISO, 2018). It included recommendations on how to accept and

handle information on possible vulnerabilities, disseminate resolution information and examples of content and was applicable to vendors who practiced vulnerability disclosure in order to reduce their risk.

2.8.5 COBIT 2019

The COBIT 2019 framework was developed by the international non-profit organisation ISACA to assist organisations in terms of information management and governance (CIO, 2019). The management practice from COBIT 2019, BAI08 Manage Knowledge stated that organisations should use and share knowledge (ISACA, 2018). In the case of VDP's, this process could be applied as researchers were sharing knowledge of the vulnerabilities with the respective vendors (Delak, 2015).

2.9 Conclusion

The chapter started with understanding what vulnerabilities and VDP's were, the types of VDP's, why VDP's were important and the challenges and benefits of VDP's. It covered cybersecurity definitions, cybercrime statistics and how VDP's fit into frameworks that touch on cybersecurity. After analysing the literature, the researcher noted that although there were some studies that cover aspects of vulnerabilities and VDP's, more research was required on the challenges and benefits of VDP's as well as whether VDP's should be implemented as part of an overall cybersecurity strategy. The next chapter will cover the theoretical framework that will be used in this study.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The literature review confirmed that there was an area of research lacking in terms of the implementation of VDP's as well the associated challenges and benefits of VDP's. Research into VDP's and the challenges and benefits of implementation will assist individuals and organisations in the understanding of VDP's and its effective implementation. Thus, confirming the importance of this research topic. In this chapter the researcher considers the research methods available and selects the most appropriate method for the study in order to correctly analyse the collected data. This chapter begins with the aim and objectives of the study. It then clarifies the theoretical framework used and discusses the research methodology, the approach, clarifies the theoretical framework used, sampling strategy, data collection and analysis methods. It also discusses the design of the questionnaire, ethical considerations and limitations of the study.

3.2 Research Aim and Objectives

Kothari (2004) stated that the main purpose of research was to discover the truth which was hidden and was not discovered yet. Based on the researcher's knowledge and experience in the cybersecurity field and the cybercrime statistics from the literature review, it was confirmed that there was a need to have a method for discovered vulnerabilities to be disclosed to organisations. The aim of this research was to explore the challenges and benefits of VDP's and the need for such a program as part of the organisational cybersecurity strategy.

The research satisfied the following research objectives:

- To determine the challenges associated with vulnerability disclosure programs.
- To determine the benefits associated with vulnerability disclosure programs.
- To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy.

3.3 Theoretical Framework

The study used the theory of planned behaviour (TPB). An article by Boston University (2019) stated that the main component of this model was the behavioural intent and behavioural intentions which were influenced by the attitude regarding the likelihood that the behaviour would have an expected outcome.

In order to guide this research, an appropriate framework had to be considered. Research in Information Technology identified theories related to technology acceptance and adoption. In the Information Technology discipline, there were theories such as the Unified Theory of Acceptance (UTAUT), the Theory Acceptance Model (TAM), and the Theory of Planned Behaviour (TPB) (Dwivedi, Rana, Jeyaraj, Clement, & Williams, 2017). The researcher considered these models for this study as VDP's were related to information technology.

The UTAUT model has been used in technology adoption since it's introduction (Williams, Rana, & Dwivedi, 2015). UTAUT suggested that the four constructs of performance expectancy, effort expectancy, social influence and facilitating conditions were direct determinants of behavioual intention and behaviour.

The TAM model evaluated an individuals intention to use a technology or system was determined by the perceived usefulness and the perceived ease of the system. According to Rauniar, Rawski, Yang, & Johnson (2014), TAM predicts an individual's adoption and voluntary use of technology.

According to the literature reviews conducted, VDP's comprised of more than technology adoption. It comprised of understanding, skills and behaviours. These attributes did not involve the adoption of any technology, instead required that a user had to decide what were the correct actions to take in order to

prevent vulnerabilities from being exploited. For this type of study, theories such as TAM and UTAUT were not suitable as understanding, skills, behaviours and actios were not considered as part of the models.

The argument above provided the motivation to search for theories that were more suitable for the study of the intentions and actions that support secure behaviour. The TPB framework, originally proposed by Icek Ajzen, is a theory that focused on the human behaviour (Boston University, 2019). It assumed that an individuals concious choice was represented by their behaviour. (Bhattacherjee, 2012). The TPB framework was used in investigating the ethical behaviour of individuals and their decision in terms of the adoption of, and compliance with, cybersecurity measures. A study by Chandarman & van Niekerk (2017) utilised an adapted TPB framework to determine the knowledge, self-perception of skills, actual skills and behaviour, and attitudes of the participants in relation to cybersecurity awareness.The TPB framework was deemed to be suitable as it investigated behaviour and the decisions taken thereof.

Elements of the Theory of Planned Behaviour (TPB)

According to the TPB model, action was guided by three kinds of variables that were critical when trying to change behaviour (Boston University, 2019).

1. Behavioural beliefs
2. Normative beliefs
3. Control beliefs

Figure 1. below illustrates the original TPB model.

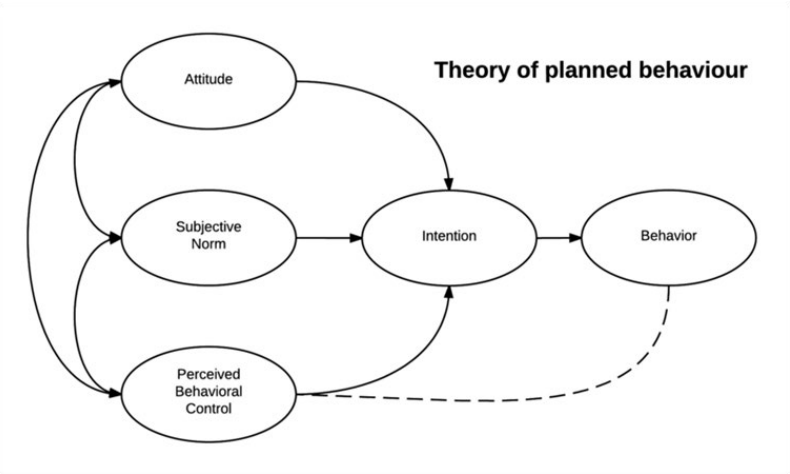

Figure 1. Original TPB Model

Source: (Boston University, 2019)

An adaption of the TPB to the study in relation to vulnerability disclosure yielded the following variables.

Figure 2. below shows the adapted version of the TPB framework

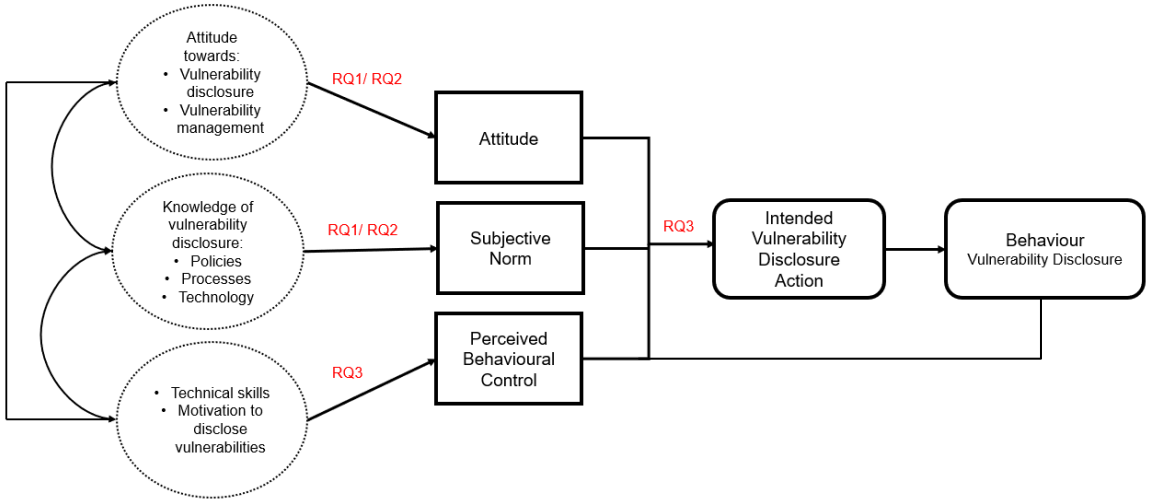

Figure 2. Adapted TPB Model

(Adapted from source (Boston University, 2019))

In this study TBP was adapted to help determine whether variables such as the attitude towards vulnerability disclosure, vulnerability management, knowledge of vulnerability disclosure policies, process and technology, technical skills and the motivation to disclose vulnerabilities affect behaviour. The choice of these factors was based on the research objectives to determine the challenges, benefits and the need to implement VDP's as part of a cybersecurity strategy. The National Telecommunications and Information Administration (2015) confirmed that the attitude of a security researcher affects the action they would take in terms of disclosing a vulnerability. A study conducted by Algarni & Malaiya (2013) confirmed that security researchers require a certain knowledge and skill in order to detect vulnerabilities. This level of skill and knowledge affected the action the security would take as well as determine the security researchers motivation for the action.

The TPB framework explored VDP's and focused on relationships amongst the following four core constructs. This framework was used to understand the challenges and benefits of VDP's and if such a program should be included in the overall organisation cybersecurity strategy.

- ***1st Construct:*** Attitude: Addressed research question 1 and 2 and assumed that the attitude in terms of VDP's, influences the action to be taken which may/ may not result in vulnerability disclosure.
- ***2nd Construct:*** Subjective norm: Addressed research question 1 and 2 and assumed that the knowledge in terms of VDP's, influences the action to be taken which may/ may not result in vulnerability disclosure.
- ***3rd Construct:*** Perceived behavioural control: Addressed research question 3 and assumed that the level of skills in terms of vulnerability discovery and exploitation, influences the action to be taken which may/ may not result in vulnerability disclosure.
- ***4th Construct:*** Intended Vulnerability Disclosure Action: Addressed research question 3 and assumed that the previous three factors influence the action taken, thus driving behaviour.

3.4 Type of Research

According to Bhattacherjee (2012), there were three types of research. These were exploratory, descriptive and explanatory and are summarised in the table 2. below.

Type of Research	Exploratory	Descriptive	Explanatory
Description	Performed in new areas of inquiry where the purpose of the research was to: 1. Gauge the extent of a phenomenon 2. Gather ideas on a phenomenon. 3. Gauge the feasibility of performing more studies of a phenomenon.	Focused on observations and documentation of a phenomenon and had to be based on scientific methods. Examined the what, where and when of a phenomenon.	Focused on the explanations of a phenomenon. It determined the factors and outcomes of a phenomenon.
Pros & Cons	**Pro:** Could be good for understanding the extent of the problem. **Con:** Could not obtain an accurate understanding of the problem.	**Pro**: More reliable than untrained observations.	**Con:** Required good interpretation and theoretical skills.

Table 2. Pros and Cons of Types of Research

Researcher compiled. Source: (Bhattacherjee, 2012)

Based on the research types listed in table 2, the most suitable type for this research was the exploratory research design. According to Bhattacherjee (2012), an exploratory research was conducted when a study had not been done in a specific area. This was done to investigate the scope, obtain preliminary designs and to determine whether there was opportunity to perform further study on the phenomenon.

The main goal of this study was to obtain an understanding of the benefits and challenges of VDP's and the need for such a program as part of the organisational cybersecurity strategy. Therefore, this design methodology was suitable to conduct this study as it created new knowledge and served as a precursor for further research. This research was a study within South Africa.

3.5 Research Approach

Research can be conducted using either qualitative or quantitative analysis. Bhattacherjee (2012) stated that qualitative analysis focused on the study of the core or underlying aspects such as feelings and reasons. The gathering, analysis and reporting of numerical data was defined as quantitative analysis. This is further outlined in the table 3. below.

Qualitative	Quantitative
Analysed qualitative data such as text from an interview.	Analysed numeric data using statistical tools.
A creative and investigative mindset was required.	Required researchers' analytical skills
Inductive reasoning	Deductive reasoning
Interviews conducted to collect data with open-ended questions	Based on questionnaires with closed-end questions

Table 3. Difference between Qualitative and Quantitative Analysis

Researcher compiled. Source: (Bhattacherjee, 2012)

Based on the characteristics listed in table 3, it can be reasoned that quantitative analysis was the most suitable for this study. This research was performed without interference from the researcher. The data was collected from a large group of participants; therefore, numeric representation of the data was the most suitable option. According to Sekaran & Bougie (2010), quantitative analysis is used for data collected through questionnaires.

3.6 Sampling Strategy

The definition of sampling by Bhattacherjee (2012), is the process of selecting a subgroup, also known as a sample from the target population for observational and purposes of deriving statistical inferences about that target population. The sampling design selected for this study was non-probability sampling. "Nonprobability sampling is a sampling technique in which some units of the population have zero chance of selection or where the probability of selection cannot be accurately determined." (Bhattacherjee, 2012, p. 69). Sekaran & Bougie (2010) also stated that non-probability sampling was used when the elements did not have a predetermined opportunity of being chosen.

This research used a nonprobability sampling using convenience sampling of the IT and cybersecurity professionals that were affiliated with the South African chapter of the international organisation Information Systems and Audit Control Association (ISACA). Convenience sampling as stated by Kothari (2004), was performed when objects in the target population were selected because of ease of access. ISACA was the largest professional organisation with cybersecurity and IT professionals as their members. Thus, ISACA South Africa was selected as the target population.

3.6.1 Sample

A sample, as defined by Trochim (2020) was a precise illustration of the target population. Sample size was the number of subjects that participated in the research. The sample used in this research was chosen from IT and cybersecurity professionals that had the knowledge of and experience with vulnerabilities.

3.6.2 Sample size

According to the sample table recommended by Sekaran & Bougie (2010), the sample size for the questionnaires that was recommended to be used in this study, was 329 respondents across ISACA South Africa at a 95% confidence level and 5% marginal error rate. However, due to the poor response rate, only 147 responses were received. According to an email delivery report received from ISACA SA, of the 2326 emails that were sent out, only 2321 were delivered and only 765 emails were opened. This was 33% of the population and it confirmed the poor response rate. This represented approximately 6.2% of the target population and 45% of the suggested sample size. ISACA SA continued to share the survey with their members on a weekly basis, via email and their social media platforms, however, limited responses were received. As a result, the target population used in this study was the 765 opened emails as it provided some assurance in terms of email delivery. This had a sample size of 256, which represented a 57% response rate in terms of the sample size. Additionally, according to Sekaran & Bougie (2013), a response rate of 30% is acceptable. Furthermore, the data collected represented 9 provinces, 13 industries and 12 different job functions across South Africa. As a result, the 147 responses were deemed suitable for this study as it provided insight into the state of VDP's within South Africa.

3.6.3 Study Site

The research was based in South Africa with the Information Technology (IT) and cybersecurity professionals affiliated with ISACA South Africa. This study site was selected as these participants may have had knowledge of vulnerabilities and VDP's as they were employed in the IT and cybersecurity fields.

3.6.4 Target Population

The target population used in this research, comprised of the Information Technology (IT) and cybersecurity professionals that were affiliated with the South African chapter of the international organisation ISACA. This was done to obtain reliable and worthwhile information. These IT and cybersecurity professionals were deemed to have had the knowledge of and experience with vulnerability disclosure programs. The target population comprised of approximately 2326 members. ISACA South Africa distributed the questionnaire via email and their social media platforms to their members.

3.7 Data collection methods

In order to the conduct this study, the research questionnaire was circulated to the target population. Bhattacherjee (2012) stated that a questionnaire was a type of research instrument that consisted of questions that was intended to obtain the responses from participants in the study in a structured manner. A questionnaire was chosen as the research instrument as it could reach participants across the provinces and industries within South Africa in a quick and efficient manner. The questionnaire was distributed by ISACA SA to their members via email and social media platforms, on a weekly basis over a month. The questionnaire measured the opinions, views and experience of the various stakeholders. The questionnaire comprised of various rating and ranking scales such as the Likert scale in order to obtain a rich and accurate data set for analysis. This instrument was suitable for quantitative analysis using the statistical analysis tools.

3.8 Data Quality Control

The data and methods used in this study, complemented each other. This assisted in improving the quality of data. The questionnaire data that was collected, was analysed and compared to maintain the reliability and validity of information. The Cronbach's Alpha coefficient was calculated in order to determine the reliability of the data.

3.9 Measurements

The questionnaire that was distributed, used closed questions and comprised of various rating and ranking scales such as the Likert scale in order to obtain a rich and accurate data set for analysis.

3.10 Data analysis

The data that was gathered through the research questionnaires, was examined using descriptive analysis (i.e.: frequency analysis, mean and standard deviation) and correlation. Singh (2006) stated that descriptive analysis was concerned with the facts and can be used over a national geographic spread at minimal costs and effort. The researcher had prior knowledge and understanding of the statistical analysis tools PSPP and Real Statistics which is an add on in Excel. As a result, these were used to analyse the data. Descriptive analysis was used in order to derive patterns and to summarise the data to determine the challenges, benefits and need for VDP's as part of a cybersecurity strategy.

Correlation analysis was also used to study "the joint variation of two or more variables for determining the amount of correlation between two or more variables." (Kothari, 2004, p. 130). These were performed to determine if there were any relationships between the questions to identify groupings or clusters, as well as to validate the responses received. The combination of the various types of analysis enabled the data to be handled in a manner that made it interpretable in accordance with the research objectives.

3.11 Design of the questionnaire

Bhattacherjee (2012) stated that a questionnaire was a type of research instrument that consisted of questions that was intended to obtain the responses from participants in the study in a structured manner. Bhattacherjee (2012) also stated that the questions must be created in such a manner that it was clear and understandable, should not be worded in a negative manner, be ambiguous, biased, contain value-laden words, too general, presumptuous, too detailed, imaginary or double-barrelled.

According to Kothari (2004), the benefits of using a questionnaire were that costs are low when the target population was geographically spread, and it offered anonymity. It was also free from bias as the respondents' answered the questionnaire themselves. The challenge with this instrument was that there was a low return rate, it was slow, control over the instrument may be lost once distributed, the approach cannot be changed once distributed, it was difficult to ascertain whether the willing participants were truly representative and there was a chance of obtaining ambiguous responses.

Each research question was used as a sub section of the research questionnaire with questions related to that section. This study used Google Forms to administer the questionnaire. A new questionnaire was created with the relevant sub sections and questions. Page logic was used in the questionnaire to terminate the questionnaire when participants did not provide consent to participate in the survey. The data was collected over a one-month period and would have taken approximately fifteen minutes to complete. Reminder e-mails were sent by ISACA South Africa every week to the target population. At the end of the one-month period, the data was exported from google forms for analysis.

The participants were not requested to submit their names as part of the questionnaire. The questionnaire assigned a unique number to each response in the database. The questionnaire comprised of a total of 27

closed questions. These were created to request participants to select responses from a list of predefined alternatives.

The questionnaire was structured into 5 sections which aligned to the objectives of the research. Each section began with a title to describe the section as outline in table 4. below. Refer to appendix 1 for the complete questionnaire.

Section	Description
Section 1	This section related to demographical information, requiring participants to provide the industry they work in, the location of the organisation, their gender, age group and current role.
Section 2	This section required participants to complete questions that provided an overview of the participants understanding of VDP's as well as their organisation's current posture.
Section 3	Aimed to determine the challenges that organisations faced in terms of implementing a VDP. It required participants to select the restrictions, determine if their organisation experienced an extortion scheme and the time frame an organisation should be allowed to fix a vulnerability.
Section 4	Aimed to determine the participants understanding of the benefits of implementing a VDP and whether it should be implemented as part of a cybersecurity strategy.
Section 5.1	Requested participants to provide the reasons for why individuals participated, why individuals feared to participate, what motivates them to discover vulnerabilities, what would they do if their discovered a vulnerability and if they had the necessary skills to discover, exploit and/ or remediate vulnerabilities.

Section	Description
Section 5.2	Focused on the intention of organisations to implement VDP's by requesting participants to provide the reasons why organisations implement VDP's, if their organisation had a VDP policy and if their organisation followed defined frameworks.

Table 4. Questionnaire Outline

The questionnaire ended with a thank you to all participants.

Table 5. below shows the linkage between the research objectives and the questionnaire.

Research Objective	Questionnaire reference
RO1: To determine the challenges associated with vulnerability disclosure programs.	Section 2, 3
RO2: To determine the benefits associated with vulnerability disclosure programs.	Section 4
RO3: To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy.	Section 5.1 and 5.2

Table 5. Linkage between Research Objectives and Questionnaire

3.12 Pre-Testing the Questionnaire

Pre-testing of the questionnaire was important to ensure that the questionnaire was structured appropriately in order to be interpreted clearly and correctly by the participants (Sekaran & Bougie, 2010). The pre-testing involved a small group of participants that were selected based on convenience, which allowed the researcher to correct any identified issues prior to collecting data. The researcher pre-tested the

questionnaire with five colleagues before having it distributed to the total population. The participants of the pre-test were requested to provide comments on the questionnaire in order to resolve any errors.

3.13 Conclusion

This chapter illustrated the importance of the research methods related to this research. It assisted the researcher in understanding the steps required to collect the data through to analysis. It began with the aim and objectives of the study. It discussed the research methodology used, the approach, analysis and sampling performed as well as the data collection strategy. It assisted the researcher in selecting the sample and selecting non-probability convenience sampling after considering the pro's and con's. The researcher could effectively administer the questionnaire and perform the appropriate analysis. The questionnaire was able to reach different provinces and industries across South Africa, as it was distributed electronically. It also covered the ethical considerations and limitations of the study. This chapter created the foundation of this research with the analysis of the data from the research instrument presented in the proceeding chapter.

CHAPTER 4 – ANALYSIS, PRESENTATION AND DISCUSSION OF THE RESULTS

4.1 Introduction

This chapter discusses the analysis of the online questionnaire data, as described in chapter 3. The results have been analysed, presented and discussed in a manner that aligns to the research objectives and questionnaire that was outlined in Chapter 1.

This research was aimed at determining the challenges, benefits of VDP's and whether VDP's should be implemented as part of a cybersecurity strategy. The results and outcomes of the analysis that are explored in this chapter are linked back to the research objectives in the sections that follow. Hence, the findings are associated to the objectives of the study that addressed the research problem. These were:

- **Research Objective 1:** To determine the challenges associated with vulnerability disclosure programs.
- **Research Objective 2:** To determine the benefits associated with vulnerability disclosure programs.
- **Research Objective 3:** To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy.

The sample for this research was selected from the cybersecurity professionals within South Africa. The questionnaire was distributed via email and social media platforms (Twitter, Facebook and LinkedIn) by the gatekeeper, ISACA South Africa, to their South African members.

The chapter highlights the percentages associated with the demographical information. It then delves into each research objective with descriptive analysis performed. It further discusses the correlation analysis performed and the assesses the reliability by using Cronbach's Coefficient Alpha. The chapter then concludes with a summary of the key findings based on the analysis.

4.2 Demographical information of the respondents

The total number of respondents for the online questionnaire was 147 across 9 provinces and 13 industries across South Africa. These respondents were requested to complete their demographical information. The demographic information that was important for this study was their industry, location, gender, age group and job role.

4.2.1 Industry of Organisation

Figure 3. below, illustrates the industry of the participants organisation. 32 (22%) of the respondents were from the *Technology, Media and Telecommunications* industry. 26 (18%) from *Financial Services*, 24 (16%) from *Retail and Consumer*, 22 (15%) from *Professional Services*, 7% from *Transportation and logistics*, *Automotive and Manufacturing* and *Government and Public Services*. 3% from *Insurance* and 1% from *Cybersecurity, Education, Entertainment, Mining and Oil and Gas*. The diversity of the industry was suitable for confirming that VDP's are not limited to technology organisations.

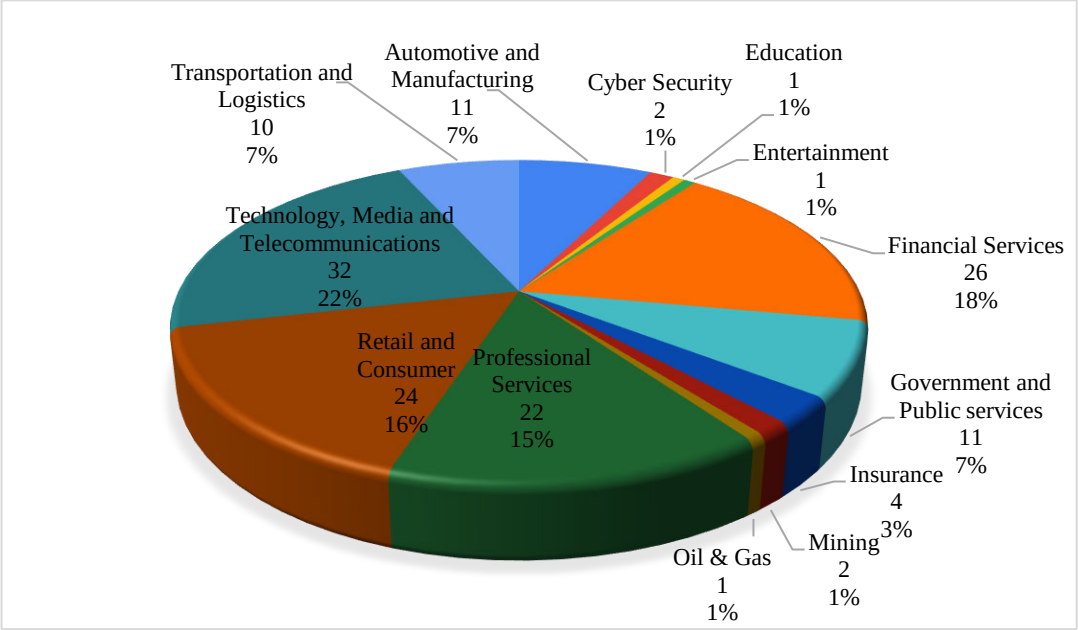

Figure 3. Industry of Organisation

4.2.2 Location of Organisation

Figure 4. illustrates the region of the respondent's organisation. Majority 77 (52%) of the respondents were from *Gauteng*, followed by *KwaZulu-Natal* with 29 (20%), *Western Cape* 21 (14%), *Mpumalanga* 6 (4%), *Eastern Cape* 5 (3%), *Northern Cape* 4 (3%), *North West* 3 (2%) and 2 shared amongst *Multinational* and *Other* with 1 respondent each.

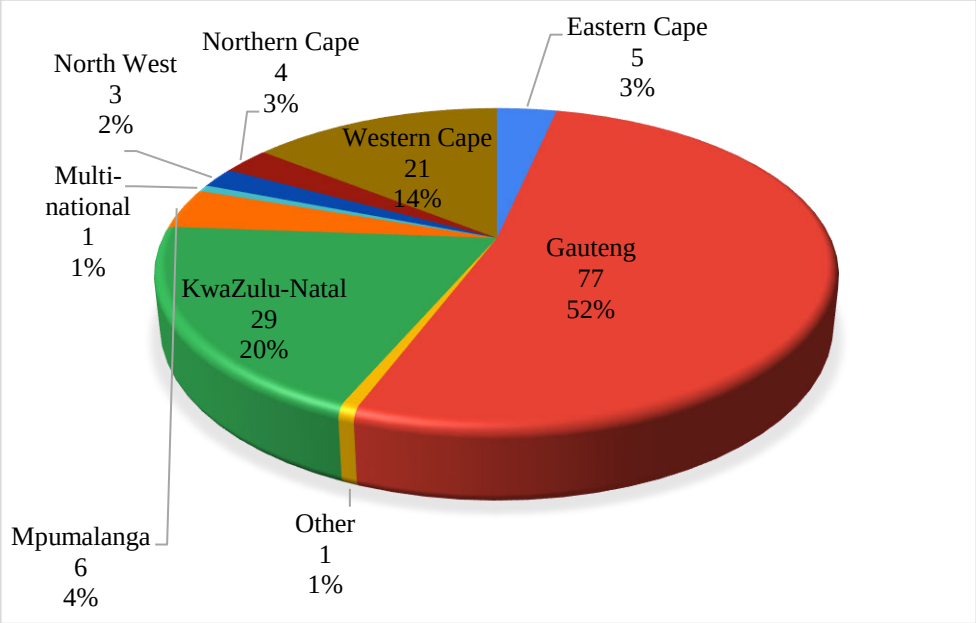

Figure 4. Location of Organisation

4.2.3 Gender

Figure 5. indicates the gender of the respondents. Majority of the respondents were *Male* 89 (61%), followed 49 (33%) *Females* and 9 (6%) who preferred not to answer.

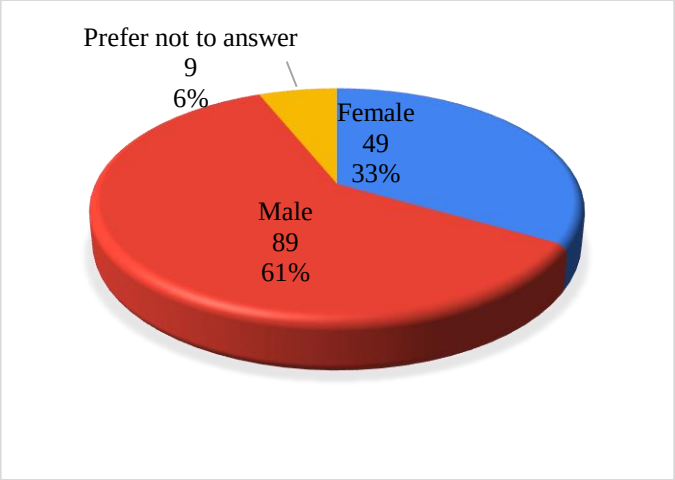

Figure 5. Gender of the participants

4.2.4 Age Group

Figure 6. illustrates the various age categories of the respondents. The majority 72 (49%) of the respondents were < *30 and* < *40 years*, 36 (24%) were >*25 and* < *30 years*, 31 (21%) were > *40 and* < *50 years*, 7 (5%) were > *50 and* < *60 years* with 1 respondent >*18 and* < *25 years* of age.

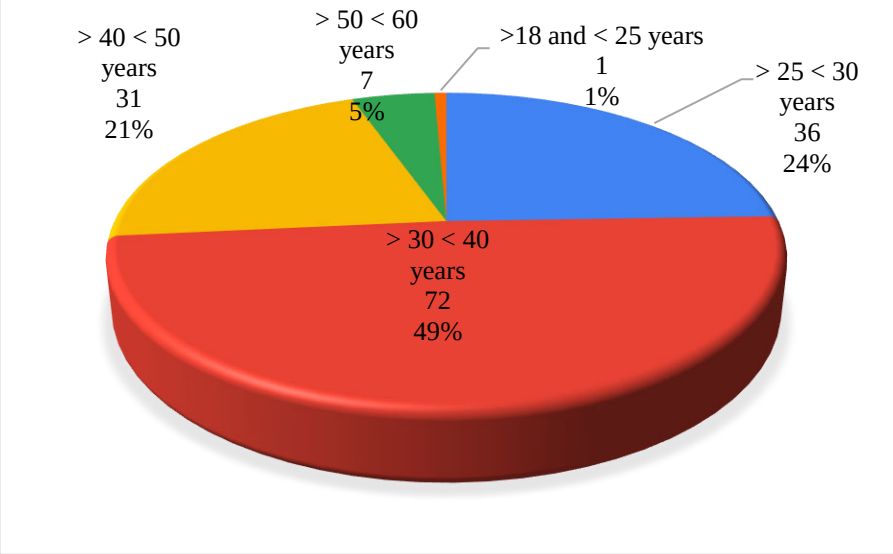

Figure 6. Age group of the participants

4.2.5 Job Functions

Figure 7. represents the job function of the respondents. The majority 88 (60%) of the respondents was shared between the *IT Auditor/ Manager* and *Security Analyst/Architect/Officer/Sales roles*. 19 (13%) were *Systems Analysts/ Administrators*, 14 (10%) were executives such as *CEO, CIO, CISO or CAE*. 7 (5%) *Software Engineers/ Developers*, 12 (8%) were shared between *Digital Forensics, Security Researcher and Consulting* and 6 (4%) shared amongst *Governance, Partner/Director, and Cybersecurity* with 2 participants each respectively. 1 respondent was a *Business analyst*. The variety of job functions were suitable as respondents have different types on interactions with VDP's based on their role within their organisations which lead to a more accurate outcome.

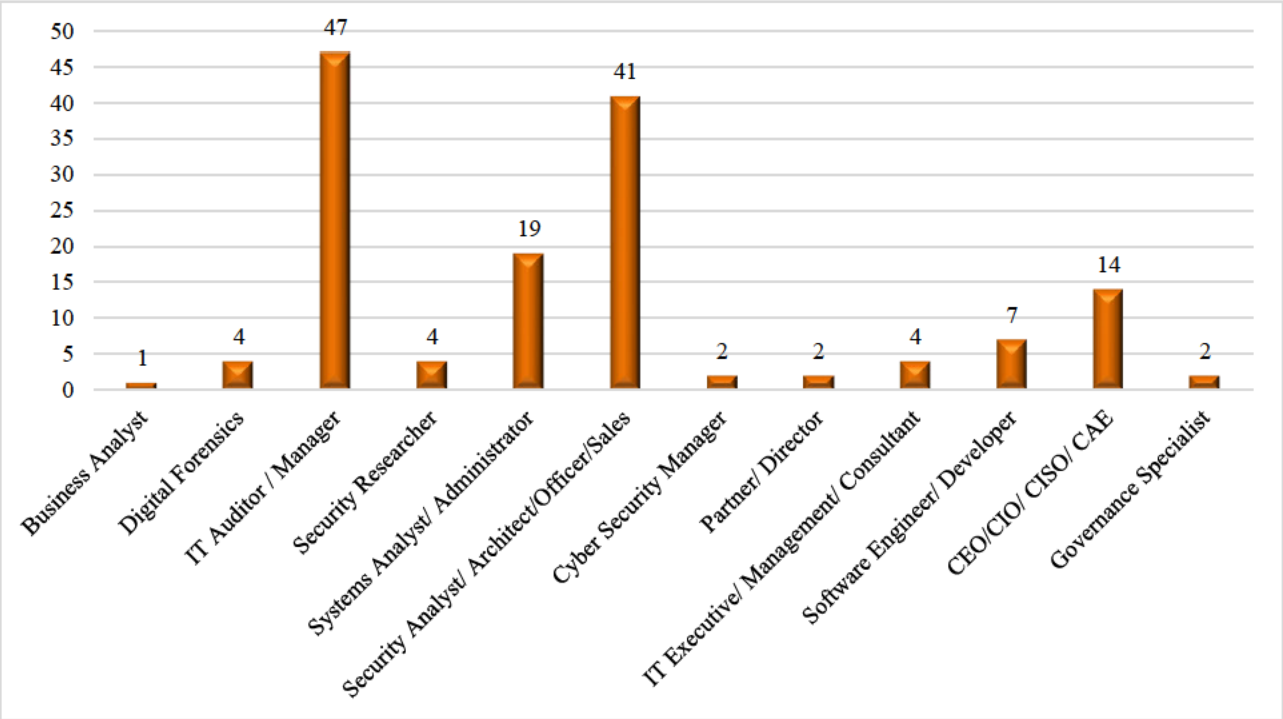

Figure 7. Job Functions of the participants

4.3 Objectives of the study

The questions in the questionnaire were linked to the research objectives to collect data that could answer each research question.

4.3.1 Research Objective 1: To determine the challenges associated with vulnerability disclosure programs

This was the first objective of the research, used to determine the challenges associated with VDP's and measured variables such as familiarity and understanding of VDP's, restrictions in implementing VDP's, time to fix a vulnerability and should a researcher wait for a fix before publishing a vulnerability.

4.3.1.1 Familiarity and Understanding of VDP's

To assess the level of understanding of VDP's, the respondents were asked to rate their understanding of VDP's, the processes associated with VDP's, the types of VDP's they are familiar with, if their organisation implemented VDP's and if VDP's are limited to technology organisations only. This related to section 2 of the questionnaire. Figure 8. illustrates the level of familiarity and understanding of VDP's.

In terms of understanding VDP's, the responses indicated that majority 93 (63%) of the respondents were *familiar with VDP's* with a mean of 3.76. 100 (68%) understood VDP's with a mean of 3.75 and 62 (42%) had an *understanding the processes associated with VDP's* with a mean of 3.24. The responses also highlighted that 47 (32%) of the responses for understanding of VDP's and 85 (58%) of the responses for understanding of the processes associated with VDP's fell into the Neutral, Disagree and Strongly Disagree categories, indicating a lack of familiarity and understanding of VDP's and the associated processes.

The responses on the types of VDP's indicated that most of the responses leaned towards *Bug bounty program*s with 120 (82%) of the responses. This confirmed literature as mentioned by Porup (2018) that

many people confused bug bounty programs with VDP's. This was followed by *Full Disclosure VDP's* with 75 (51%), *Responsible-Disclosure VDP's* with 79 (54%), *Self-Disclosure VDP's* with 41 (28%) and *Non-Disclosure VDP's* with 73 (50%) of the responses. The low response for *self-disclosure* confirmed the global public vulnerability research report, where only 2% of reported vulnerabilities were self-disclosed (Frost & Sullivan, 2018). The results also indicated that there was a lack of awareness and understanding of the different types of VDP's as 106 (72%) of the responses ranged between Neutral and Strongly Disagree for *Self-Disclosure VDP's*, 74 (50%) for *Non-Disclosure VDP's*, 72 (49%) for *Full Disclosure VDP's* and 68 (46%) for *Responsible-Disclosure*.

In this section of the questionnaire the respondents were also asked about their organisations use of VDP's. 116 (79%) of the respondents fell between the Neutral to Strongly Disagree category, indicating that VDP's were not likely to be implemented within the organisation or they had no knowledge of VDP's within the organisation. Only 31 (21%) mentioned that their organisation had implemented a VDP.

Respondents were also asked if their organisation had *an official channel to disclose vulnerabilities in products and services*. 116 (79%) fell into the Neutral to Strongly Disagree category, indicating that no channel for reporting vulnerability within the organisation was available. Only 31(21%) mentioned that a channel was available. This confirmed the literature review whereby very few South African companies have implemented VDP's.

The last question of this section asked the respondents if they felt that *VDP's were only for technology organisations*. 137 (93%) of the respondents were in the Neutral to Strongly Disagree category indicating that VDP's are for all types of organisations. Only 10 (7%) felt that it was limited to technology organisations.

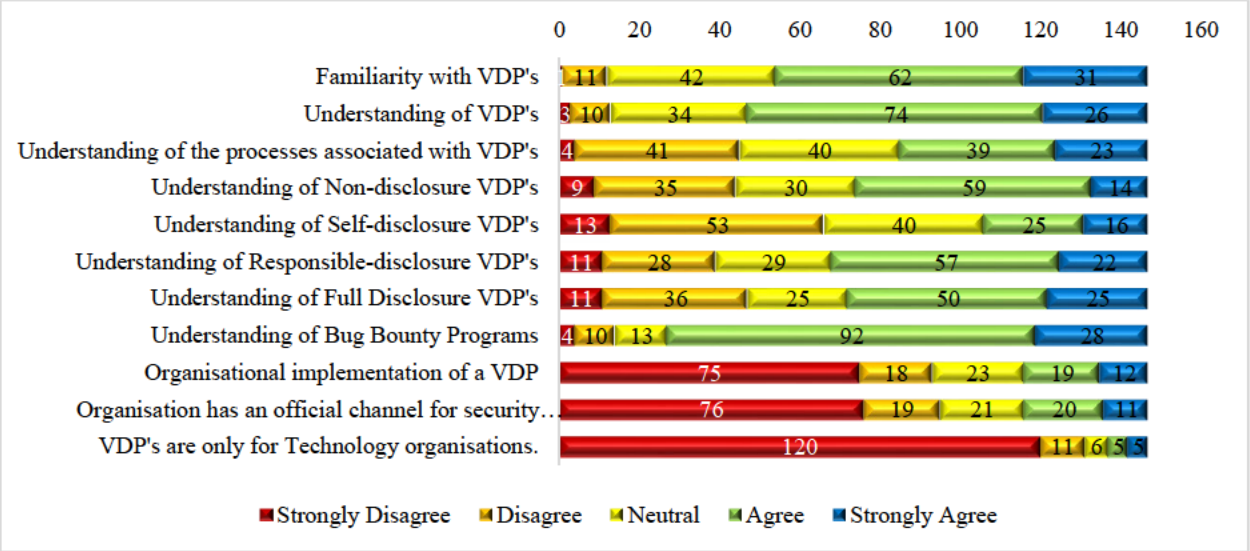

Figure 8. Understanding of VDP's

In order to create the descriptive statistics, the responses were classified from "1", Strongly Disagree to "5", Strongly Agree. Table 6. below illustrates the full descriptive analysis of the understanding of the respondents from Strongly Disagree to Strongly Agree.

	Familiarity with VDP's	Understanding of VDP's	Understanding of the processes associated with VDP's	Understanding of Non-disclosure VDP's	Understanding of Self-disclosure VDP's	Understanding of Responsible-disclosure VDP's	Understanding of Full Disclosure VDP's	Understanding of Bug Bounty Programs	Organisational implementation of a VDP	Organisation has an official channel for security researchers to disclose VDP's are only for Technology organisations.
Mean	3.76	3.75	3.24	3.23	2.85	3.35	3.29	3.88	2.15	2.12	1.39
Standard Error	0.07	0.07	0.09	0.09	0.09	0.10	0.10	0.07	0.11	0.11	0.08
Median	4	4	3	3	3	4	4	4	1	1	1
Mode	4	4	2	4	2	4	4	4	1	1	1
Standard Deviation	0.90	0.90	1.11	1.10	1.14	1.17	1.22	0.89	1.38	1.37	0.97
Sample Variance	0.80	0.81	1.23	1.22	1.31	1.37	1.49	0.79	1.91	1.88	0.94
Kurtosis	-0.29	0.66	-1.02	-0.85	-0.70	-0.76	-1.05	2.16	-0.80	-0.76	6.00
Skewness	-0.36	-0.75	0.08	-0.32	0.38	-0.42	-0.24	-1.32	0.79	0.81	2.61
Confidence Level (95.0%)	0.15	0.15	0.18	0.18	0.19	0.19	0.20	0.14	0.23	0.22	0.16

Table 6. Frequency and descriptive statistics of understanding of VDP's

The 95% confidence level for the familiarity with VDP's was 0.15. This indicated that with a 95% confidence, the population mean was between 3.61 (mean – confidence = 3.76 – 0.15 = 3.61) to 3.90 (mean + confidence = 3.76 + 0.15 = 3.90), illustrating that a positive level *(Agree)* of familiarity with VDP's. The 95% confidence levels for understanding of VDP's was 0.15 with a population mean between 3.60 to 3.89 and the understanding of the processes associated with VDP's was 0.18. The population mean was between 3.06 to 3.43, leaning towards a *Neutral to Agree* understanding of VDP's and the associated processes.

*Bug bounty program*s was the most common amongst the respondents with a 95% confidence level of 0.14 and a population mean between 3.74 to 4.03, illustrating that bug bounties was well known amongst the respondents, leaning towards *Agree*.

In terms of the organisation the 95% confidence level for the respondent's organisations implementing VDP's was 0.23 with a population mean between 1.92 to 2.37. This indicated the low level on implementation of VDP's in organisations, leaning towards *Disagree*. Respondents were also asked if they felt VDP's were for technology organisations only, the 95% confidence level was 0.16 with a population mean between 1.24 to 1.55. This showed that many believed that VDP's were not only for Technology organisations and should be implemented across industries, leaning towards *Strongly Disagree.*

Overall, it can be seen that there was a lack of understanding of VDP's and the associated processes.

4.3.1.2 Restrictions of VDP's

Figure 9. illustrates the restrictions that the respondents felt play a role in the implementation of VDP's. From the responses, the top three restrictions that were likely to impact the implementation of VDP's were a lack of understanding of VDP's with 133 (91%) responses and with a mean of 4.26, *Lack of management support* with 129 (88%) and a mean of 4.09 and a *lack of technical resources* with 115 (78%) and a mean of 3.95, all leaning towards a Agree. These results confirmed the literature by Cencini, Yu, & Chan (2005) that stated that the associated costs of VDP's outweighed the benefits.

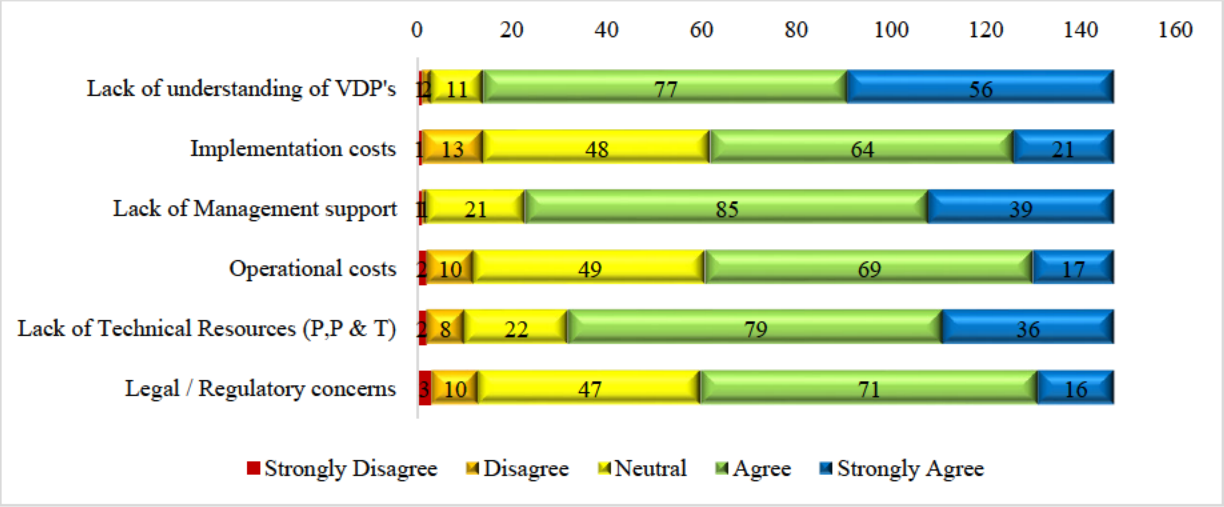

Figure 9. Restrictions associated with VDP's

4.3.1.3 Organisation was a target of a vulnerability extortion scheme

Figure 10. indicates whether the respondent's organisation was part of an extortion scheme due to discovered vulnerability. Most of the respondents leaned towards Disagree as 78 (53%) Strongly Disagreed, 19 (13%) Disagreed and 25 (17%) were Neutral. The overall mean was 2.03 leaning towards Disagree. Only a small percentage responded with Agree to this question indicating that organisational confidentiality policies could have been restricting a true response. These responses confirmed literature by PwC that stated that victims of cyber-crime lost approximately R2.2 billion a year due to cyber-attacks PwC (2018). These could have been related to unresolved vulnerabilities.

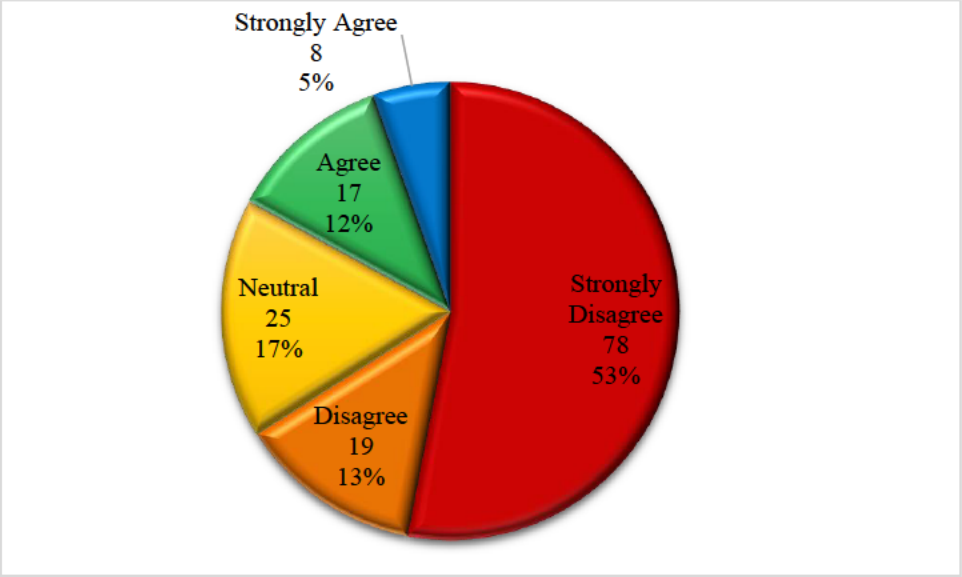

Figure 10. Organisations as part of an extortion scheme

4.3.1.4 Timeframe for fixing vulnerabilities

Figure 11. represents what respondents felt was the appropriate timeframe for an organisation to have in order to fix a vulnerability. 87 (59%) respondents felt that *>30 days and < 60 days* was the most appropriate timeframe with 70 (48%) responding with Agree and 17 (12%) with Strongly Agree. The mean for this question was 3.52, leaning towards Agree. 139 (95%) felt that an organisation should publish a vulnerability with 101 (69%) responding with Strongly Disagree, 19 (13%) with Disagree and 19 (13%) with Neutral, with a mean of 2.54, leaning towards Disagree. As per literature, organisations took too long to fix a vulnerability (Barker, 2015). According to Miller (2019), the Department of Homeland Security issued a

directive that vulnerabilities should be fixed in 30 days, confirming the response timeframe.

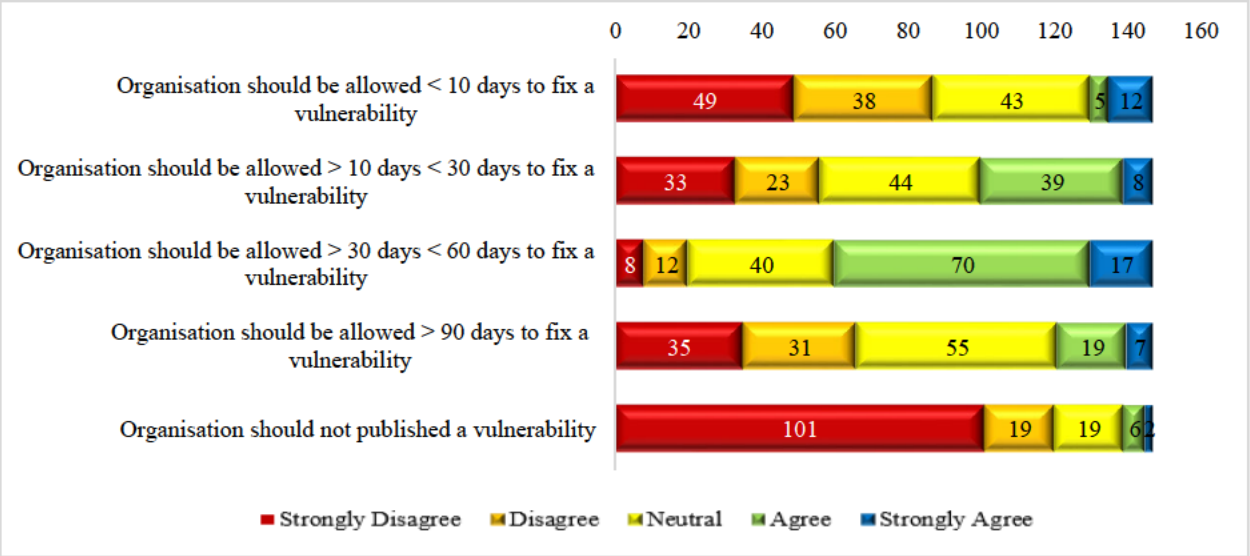

Figure 11. Timeframe for fixing vulnerabilities

4.3.1.5 Researchers should wait for a fix from a vendor

The respondents were asked whether a researcher should wait for a fix to become available by the vendor before making a vulnerability public. Figure 12. illustrates the respondent's answers. Majority of the respondents felt that a researcher should wait for fix before publishing a vulnerability with 67 (46%) answering with Agree and 47 (32%) with Strongly Agree. The overall mean for this question was 3.99, leaning towards Agree.

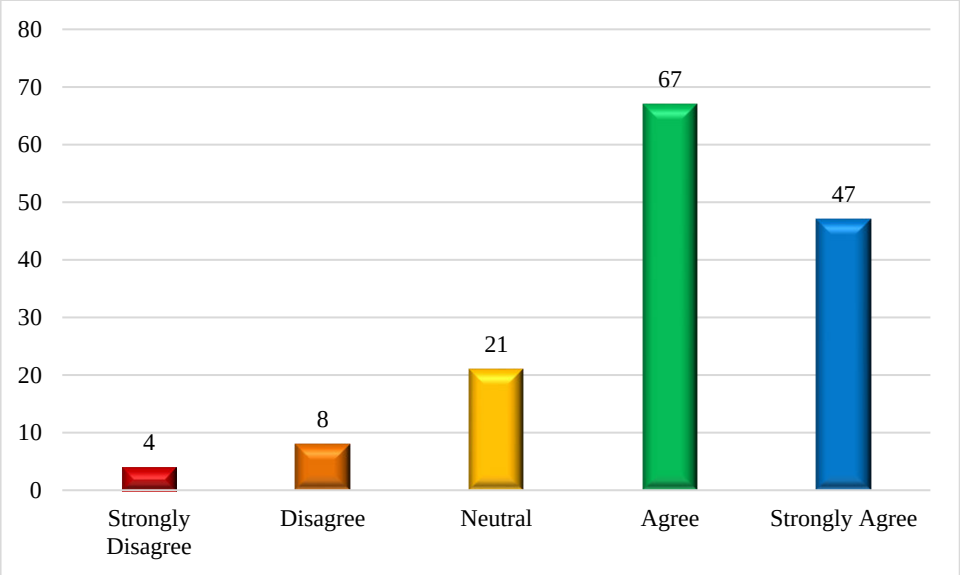

Figure 12. Vendor disclosure of a fix

Table 7. below illustrates the full descriptive statistics performed on the responses for the figures in 4.4. The responses were classified from "1", Strongly Disagree to "5", Strongly Agree.

The 95% confidence levels for the top three restrictions are 0.12 for *Lack of understanding of VDP's*, 0,12 for *Lack of management support* and 0.14 for *Lack of technical resources*. This indicated that with 95 % confidence, the population means for each of the above are *Lack of understanding of VDP's* with a population mean of between 4.14 (mean – confidence = 4.26 – 0.12 = 4.14) to 4.37 (mean + confidence = 4.26 + 0.11 = 4.37), leaning towards *Agree*, *Lack of management support* with population mean between 3.97 to 4.20, leaning towards *Agree* and *Lack of technical resources* with population mean between 3.81 to 4.09, leaning towards Agree.

	Lack of understanding of VDP's	Implementation costs	Lack of Management support	Operational costs	Lack of Technical Resources (P, P & T	Legal / Regulatory concerns	Organisation was a target of a vulnerability extortion scheme	Organisation should be allowed < 10 days to fix a vulnerability	Organisation should be allowed > 10 days < 30 days to fix a vulnerability	Organisation should be allowed > 30 days < 60 days to fix a vulnerability	Organisation should be allowed > 90 days to fix a vulnerability	Organisation should not publish a vulnerability	Researchers should wait for a fix to become available by a vendor
Mean	4.26	3.62	4.09	3.61	3.95	3.59	2.03	2.27	2.77	3.52	2.54	1.56	3.99
Standard Error	0.06	0.07	0.06	0.07	0.07	0.07	0.11	0.10	0.10	0.08	0.09	0.08	0.08
Median	4	4	4	4	4	4	1	2	3	4	3	1	4
Mode	4	4	4	4	4	4	1	1	3	4	3	1	4
Standard Deviation	0.71	0.86	0.70	0.83	0.86	0.85	1.29	1.20	1.22	0.99	1.13	0.96	0.97
Sample Variance	0.51	0.74	0.49	0.69	0.74	0.72	1.66	1.43	1.49	0.98	1.28	0.92	0.93
Kurtosis	2.73	-0.21	1.84	0.38	1.24	0.63	-0.52	-0.11	-1.08	0.47	-0.68	1.85	1.15
Skewness	-1.11	-0.28	-0.73	-0.45	-0.95	-0.60	0.89	0.75	-0.12	-0.80	0.18	1.63	-1.09
Confidence Level (95.0%)	0.12	0.14	0.11	0.14	0.14	0.14	0.21	0.20	0.20	0.16	0.18	0.16	0.16

Table 7. Frequency and descriptive statistics of challenges of VDP's

4.3.1.6 Role and Familiarity with VDP's

Figure 13. illustrates how the roles of the respondents related to their familiarity with VDP's. It was evident that respondents from the security field such as *Security analysts, architects, Officers and Sales Consultants* were more familiar with VDP's with 37 (25%) of the respondents positively responding. 33 (23%) of the negative responses were from the IT Audit field indicating a lack of awareness.

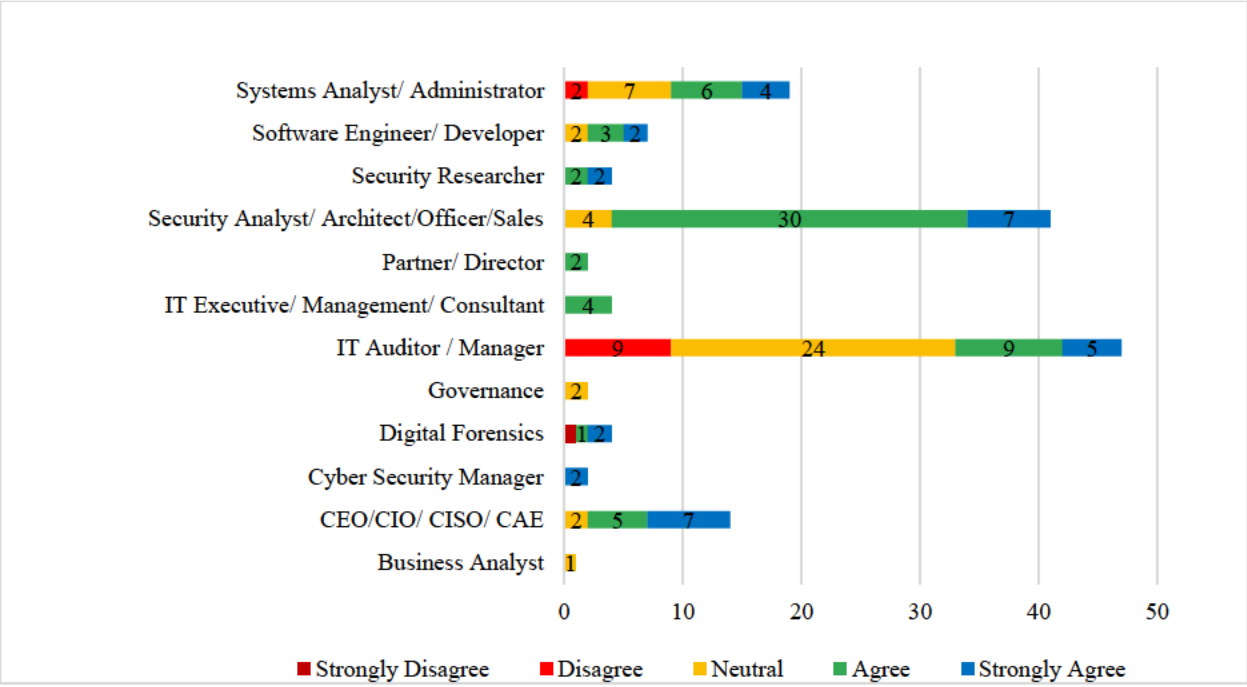

Figure 13. Role and Familiarity with VDP's

4.3.1.7 Role and Understanding of VDP's

Figure 14. represents the respondent's role and the relationship to their understanding of VDP's. Positive results were received from the Security space with *Security analysts, architects, Officers and Sales Consultants* as majority 34 (23%). This was followed by *IT Auditor/Manager* with 26 (18%), which contradicts the familiarity percentage of IT Auditor/Managers.

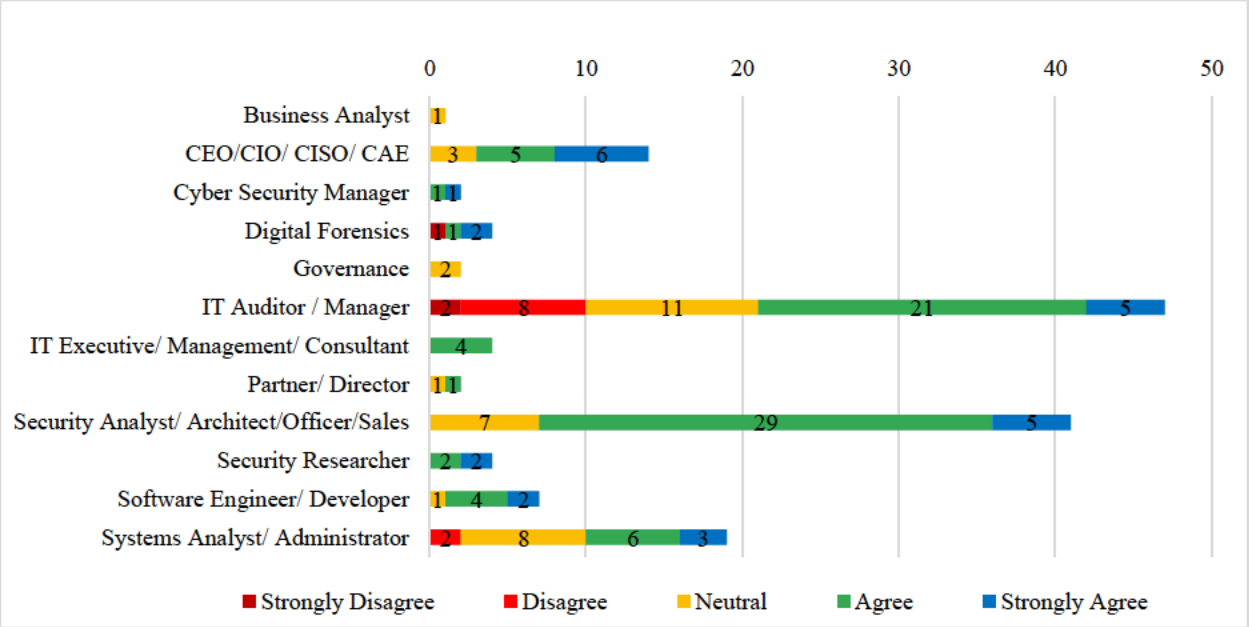

Figure 14. Role and Understanding of VDP's

4.3.1.8 Industry and Organisations that have implemented a VDP

Figure 15. illustrates the industry of organisations that have implemented a VDP. The results indicated that very few South African companies have implemented VDP's, as confirmed by research of literature, online searches and company online profiles. *Technology, Media and Communications* is a leader in terms of VDP implementation with 15 (10%) positive responses, this was followed by *Financial Services* with 5 (3%) and *Retail and Consumer* with 3 (2%). The poor rate of positive responses indicated a lack of awareness of VDP's across industries.

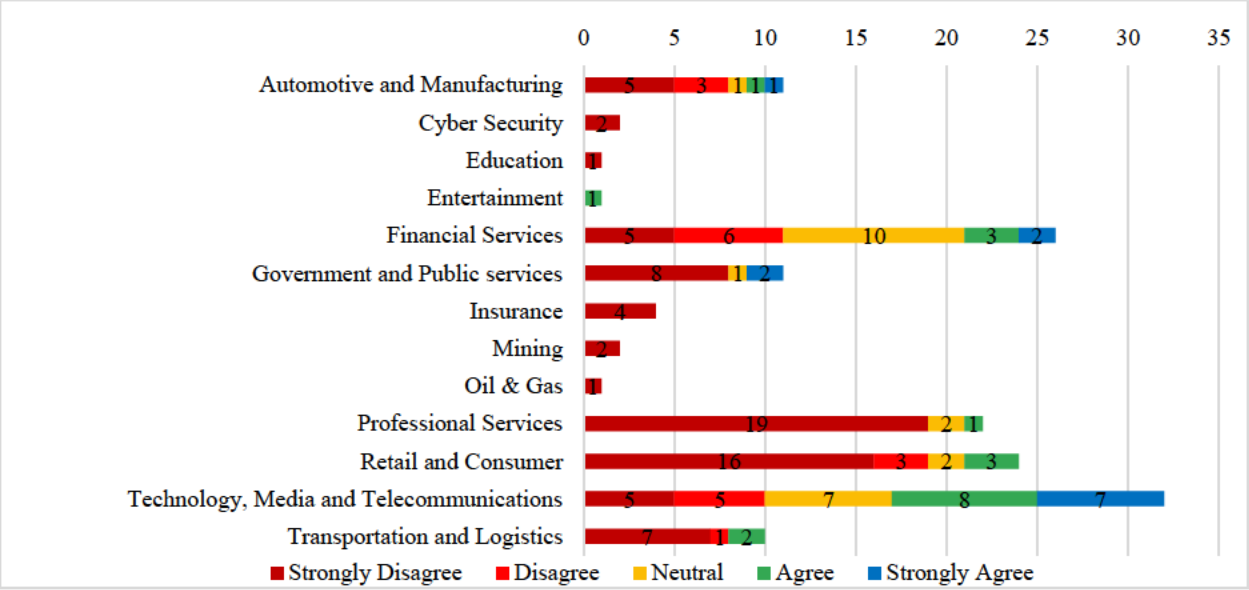

Figure 15. Industry and Organisations that have implemented a VDP

4.3.1.9 Industry and organisations that have a channel to report vulnerabilities

Figure 16. illustrates the industry of organisations that may not have implemented a VDP but has a channel for reporting vulnerabilities. The results again indicated that very few South African companies have implemented a channel for reporting vulnerabilities. *Technology, Media and Communications* was a leader in terms of a reporting channel with 16 (11%) positive responses, this was followed by *Financial Services* with 6 (4%) and *Retail and Consume*r with 2 (1%). The poor rate of positive responses indicated a clear lack of awareness of VDP's across industries and supported 4.3.1.8 above. Research conducted by Porup (2018) stated that 94% of the Forbes global companies had no channel for security researchers to report vulnerabilities, which was confirmed by the surveyed responses.

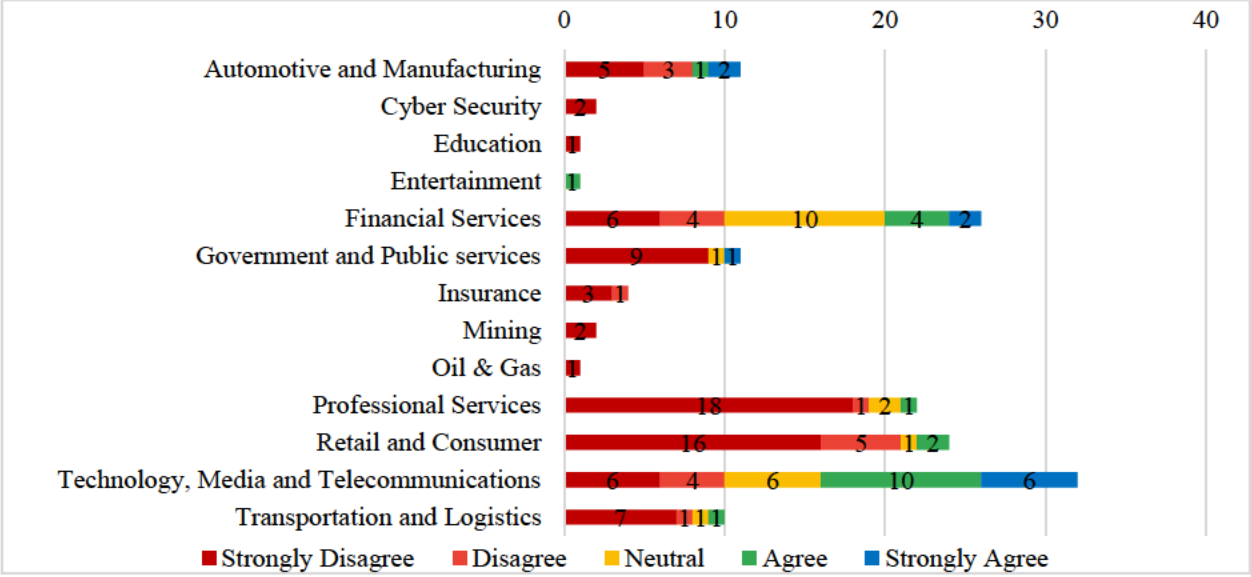

Figure 16. Industry and organisations that have a channel to report vulnerabilities

4.3.1.10 Industry and organisations that have been made a target of extortion

Figure 17. illustrates the industries of the organisations that have been a target of an extortion scheme due to a discovered vulnerability. *Technology, Media and Telecommunications* has been made target of extortion with 11 (8%) responses, followed by *Financial Services* with 6 (4%) and *Automotive and Manufacturing* with 3 (2%). It was worth noting that some organisations have confidentiality clauses, as such respondents may not have been allowed to divulge such information. The information at hand suggested that incidents due to vulnerabilities have occurred within South Africa across industries, illustrating the need for VDP's. The report by the Ponemon Institute (2019), confirmed that 60 percent of the respondents stated that one or more of these incidents could have occurred because a patch that was available for a known vulnerability, had not been applied. VDP's could have assisted in the detection of these vulnerabilities before exploitation.

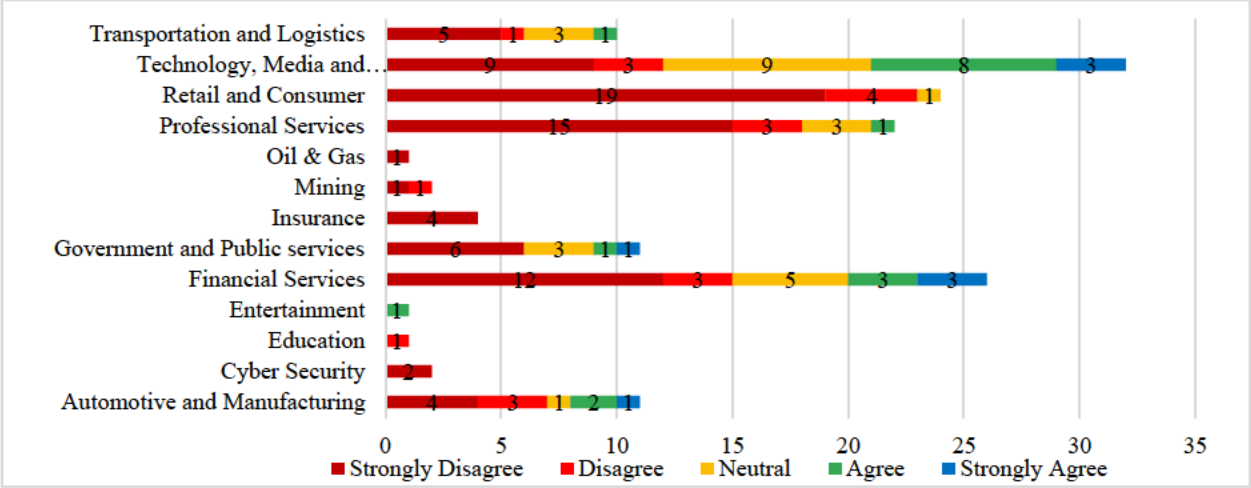

Figure 17. Industry and organisations that have been made a target of extortion

Overall, is can be seen from the responses that across industries there was a lack of understanding of VDP's and the associated processes. There were also not many organisations that implemented VDP's or had a channel to report vulnerabilities.

4.3.2 Research Objective 2: To determine the benefits associated with vulnerability disclosure programs.

This section addresses the research objectives in terms of the benefits experienced with VDP's and is section 4. of the questionnaire. It assesses variables such as the benefits of VDP's and whether it should be implemented as part of a cybersecurity strategy.

4.3.2.1 Benefits of implementing a VDP

Figure 18. illustrates the benefits that the respondents felt play a role in the implementation of VDP's. From the responses, the top three benefits that were likely to impact the implementation of VDP's were *Improved security posture* 137 (93%) with a mean of 4.44, *Reduces risk* 134 (91%) with a mean of 4.33 and an *Increase in cybersecurity awareness* 123 (84%) with a mean of 4.13, all leaning towards a Strongly

Agree. Research confirmed that improvement in the cybersecurity posture was a benefit of VDP's (Cencini, Yu, & Chan , 2005). Vidstrom (2002) stated that VDP's helped developers to create patches faster to prevent exploitation, confirming the responses in terms of reducing risk.

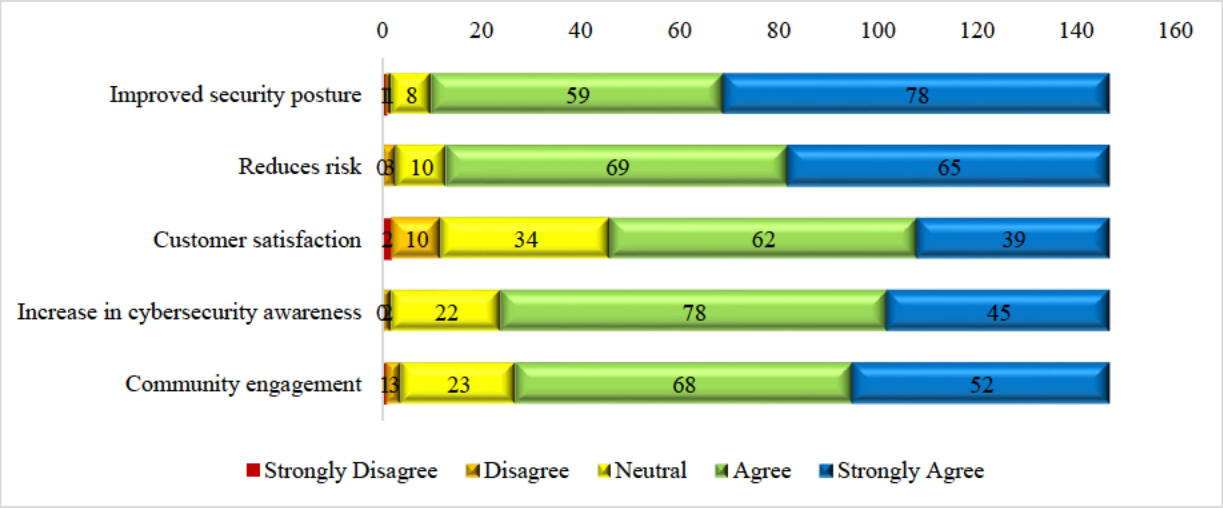

Figure 18. Benefits of VDP's

4.3.2.2 VDP's should be implemented as part of a cybersecurity strategy

Figure 19. indicates what the respondents felt about VDP's being implemented as part of a cybersecurity strategy. Majority of the respondents felt that *VDP's should be a part of a cybersecurity strategy* with 65 (44%) responding with Agree and 61 (42%) with Strongly Agree. The overall mean was 4.27, leaning towards Strongly Agree.

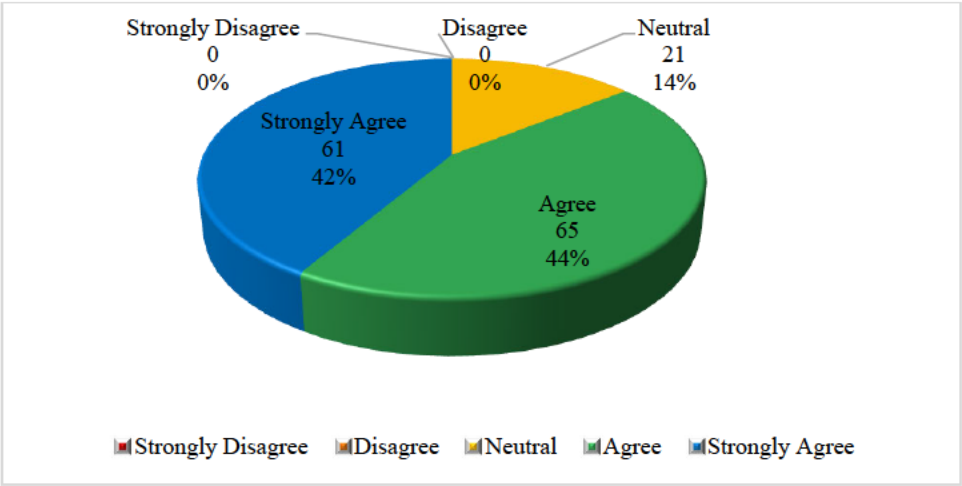

Figure 19. VDP's as part of a cybersecurity strategy

Table 8. below illustrates the full descriptive statistics performed on the responses for the figures in 4.5. In order to create the descriptive statistics, the responses were classified from "1", Strongly Disagree to "5", Strongly Agree.

The 95% confidence levels for the top three benefits are 0.11 for *Improved security posture*, 0,11 for *Reduces risk* and 0.11 for *Increase in cybersecurity awareness*. This indicated that with 95% confidence, the population means for each of the above are *Improved security posture* with a population mean of between 4.33 (mean – confidence = 4.44 – 0.11 = 4.33) to 4.56 (mean + confidence = 4.44 + 0.11 = 4.55) , leaning towards *Agree*, *Reduces risk* with population mean between 4.22 to 4.45, leaning towards *Agree* and *Increase in cybersecurity awareness* with population mean between 4.01 to 4.24, leaning towards *Agree*. This indicated that the participants were familiar with the benefits of VDP's.

	Improved security posture	Reduces risk	Customer satisfaction	Increase in cybersecurity awareness	Community engagement	VDP's should be implemented as part of the overall cybersecurity strategy
Mean	4.44	4.33	3.86	4.13	4.14	4.27
Standard Error	0.06	0.06	0.08	0.06	0.07	0.06
Median	5	4	4	4	4	4
Mode	5	4	4	4	4	4
Standard Deviation	0.69	0.70	0.94	0.70	0.80	0.70
Sample Variance	0.48	0.48	0.88	0.50	0.64	0.49
Kurtosis	3.73	1.03	0.07	-0.09	0.90	-0.88
Skewness	-1.47	-0.93	-0.62	-0.43	-0.82	-0.43
Confidence Level (95.0%)	0.11	0.11	0.15	0.11	0.13	0.11

Table 8. Frequency and descriptive statistics of benefits of VDP's

4.3.2.3 Industry and VDP's as part of cybersecurity strategy

Figure 20. illustrates how the industries related to VDP's being implemented as part of a cybersecurity strategy. The top three positive responses were received in terms of 31 (21%) responses were from *Technology, Media and Telecommunications*, followed by *Financial services* 25 (17%) and *Retail and Consumer* with 20 (14%). This confirmed that VDP's were not just for technology organisations and the need was evident across industries.

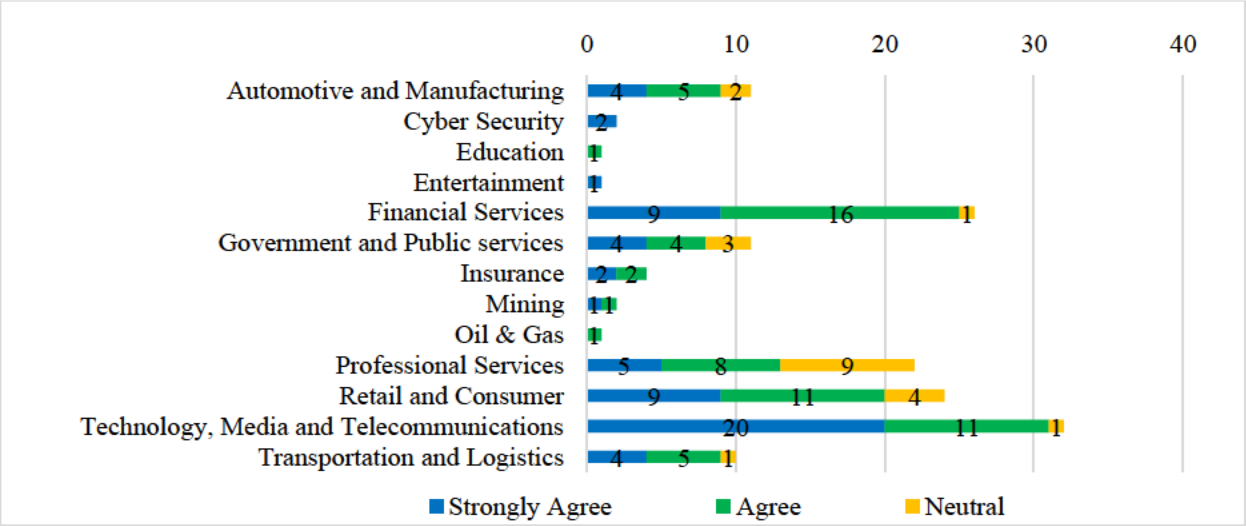

Figure 20. Industry and VDP's as part of cybersecurity strategy

The responses were indicative of what participants believed were the benefits of implementing VDP's and that VDP's should be implemented as part of a cybersecurity strategy.

4.3.3 Research Objective 3: To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy.

This section addresses the research objectives in terms of the intention of individuals and organisations to participate in VDP's and is section 5 of the questionnaire. This section aims to determine whether intention drives the success of the VDP's in a cybersecurity strategy.

4.3.3.1 Reasons why individual Intention to participate in VDP's

Figure 21. represents the respondent's feedback in terms of what they felt were the reasons individuals participate in VDP's. The top three intentions were for *monetary reasons* with 73 (50%) responding with Agree and 55 (37%) Strongly Agree and a mean of 4.16. This was followed by *Fame and Prestige* with 73 (50%) responding with Agree and 50 (34%) with Strongly Agree and a mean of 4.10. Lastly *Career advancement* with 74 (50%) responding with Agree and 32 (22%) with Strongly Agree and a mean of 3.89. The means of the three intentions mentioned above lean towards Agree. It was further noted that 127 (86%) did not feel that an individual's intent to participate in VDP's was malicious with 86 (59%) responding with Strongly Disagree, 28 (19%) with Disagree and 12 (8%) with Neutral and a mean of 1.80, leaning towards Disagree. As per literature, rewards were important to VDP participants, confirming the responses received (National Telecommunications and Information Administration, 2015).

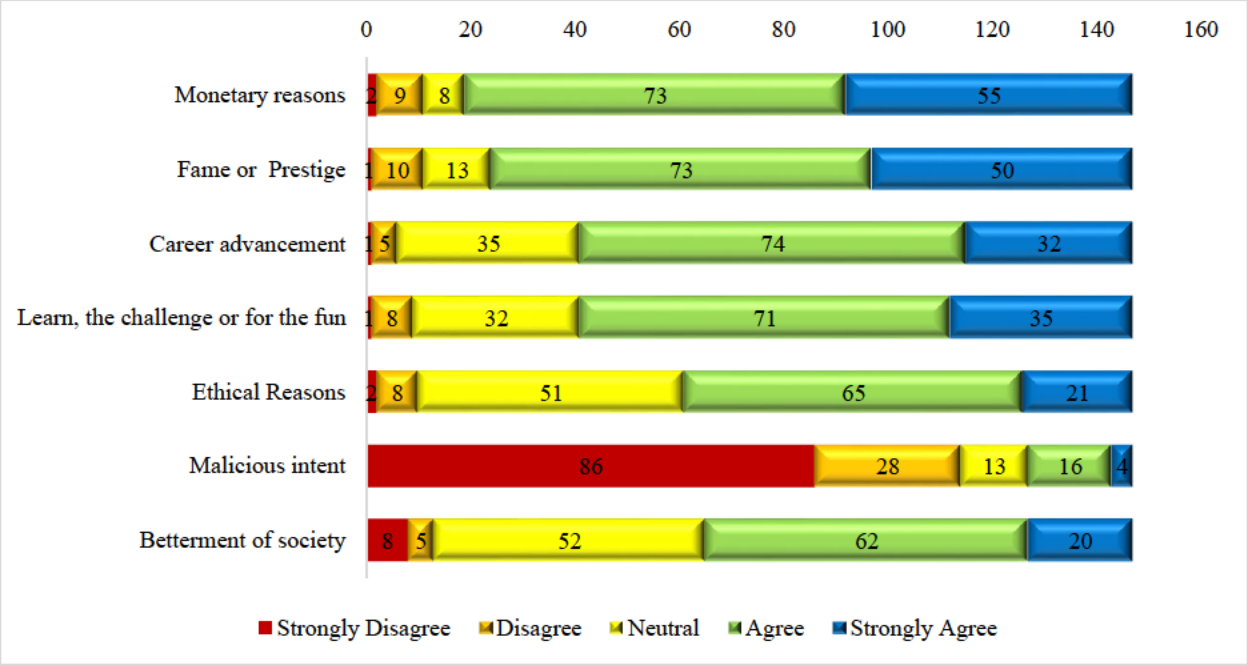

Figure 21. Reasons why individuals participate in VDP's

4.3.3.2 Reasons why individuals do not participate in VDP's

The respondents were asked what they felt were the reasons why individuals did not participate in VDP's. Figure 22. illustrates the responses. Majority 132 (90%) indicated with *Fear of punishment* with 70 (48%) responding with Agree and 62 (42%) with Strongly Agree and a mean of 4.27. This was followed by *Legal concerns* with 69 (47%) responding with Agree and 41 (28%) with Strongly Agree and a mean of 3.99, *Poor vendor communication* with 59 (40%) responding with Agree and 25 (17%) with Strongly Agree and a mean of 3.61 and Poor/ lack of VD platforms with 43 (29%) responding with Agree and 26 (18%) with Strongly Agree and a mean of 3.48. The means of the above-mentioned reasons lean towards Agree. Research confirms of the responses in terms of *Fear of punishment* as well as *Poor vendor communication*. Researchers would also like to be part of the vulnerability mitigation process. (National Telecommunications and Information Administration, 2015).

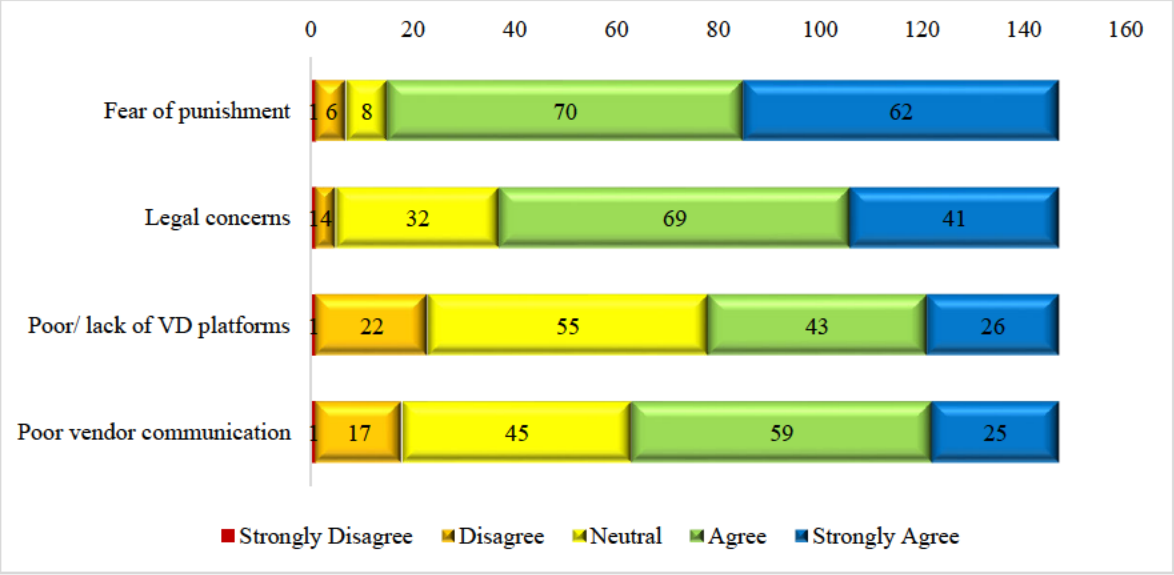

Figure 22. Reasons why individuals do not participate in VDP's

4.3.3.3 Motivation of individuals to participate in VDP's

The respondents were asked what they felt were the motivators for individuals to participate in VDP's. Figure 23. illustrates these responses. The top three motivators were for *monetary reasons* with 72 (49%) responding with Agree and 54 (37%) Strongly Agree and a mean of 4.10. This was followed by *to earn an*

item/ gift with 68 (46%) responding with Agree and 45 (31%) with Strongly Agree and a mean of 3.96. Lastly *General software security* with 69 (47%) responding with Agree and 33 (22%) with Strongly Agree and a mean of 3.84. The means of the three intentions mentioned above lean towards Agree. It was further noted that 133 (91%) did not feel that an individual's intent to participate in VDP's was malicious with 116 (79%) responding with Strongly Disagree, 11 (6%) with Disagree and 6 (4%) with Neutral and a mean of 1.48, leaning towards Strongly Disagree. 117 (%) did not feel that an individual's intent to participate in VDP's was *hacking for fun* with 98 (67%) responding with Strongly Disagree, 14 (10%) with Disagree and 5 (3%) with Neutral and a mean of 1.83, leaning towards Disagree. The findings of this section linked back to 4.3.3.1, whereby the intention and motivation to participate were associated.

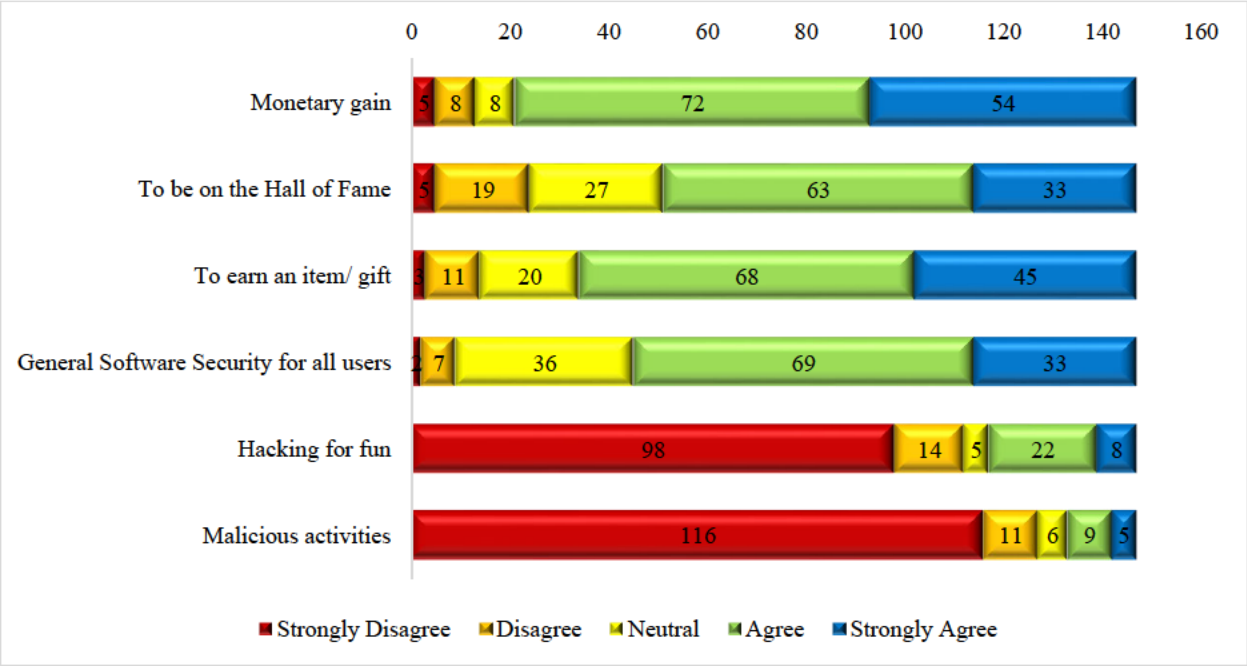

Figure 23. Motivators to participate in VDP's

4.3.3.4 Action taken if a vulnerability is discovered

Figure 24. highlights the action the respondent would take if they were to discover a vulnerability. 114 (78%) stated that they would *disclose the vulnerability to the software vendo*r with 51 (35%) responding with Agree and 63 (43%) with Strongly Agree and a mean of 4.18, leaning towards Agree. 139 (95%) stated

that they would *not ignore a discovered vulnerability* with 83 (56%) responding with Strongly Disagree and 23 (16%) with Disagree, 33 (22%) with Neutral and a mean of 1.80, leaning towards Disagree. 139 (95%) stated that *they would not keep a vulnerability secret and use it for malicious activities* with 128 (87%) responding with Strongly Disagree and 7 (5%) with Disagree, 4 (3%) with Neutral and a mean of 1.29, leaning towards Strongly Disagree.

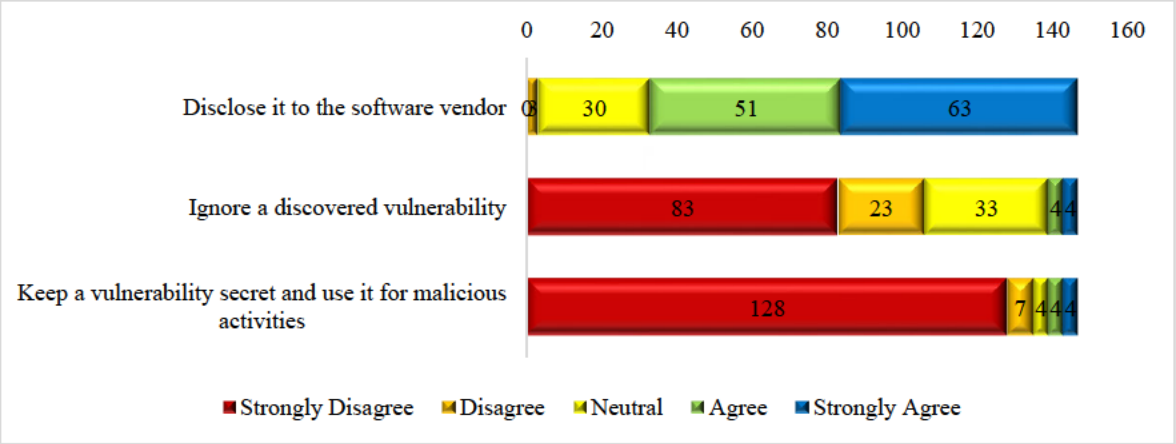

Figure 24. Action taken for discovered vulnerability

4.3.3.5 Skill level of the respondents to discover, exploit and/or remediate vulnerabilities

Figure 25. illustrates the skill level of the respondent to discover a vulnerability, exploits and/or remediate vulnerabilities. Majority of the respondents 84 (57%) responded that they did not have the necessary skills with 9 (6%) responding with Strongly Disagree, 26 (18%) with Disagree and 49 (33%) with Neutral. 63 (43%) stated that they have the necessary skills with 46 (31%) responding with Agree and 17 (12%) with Strongly Agree. The overall mean was 3.24, leaning towards Neutral, indicating an average level of skills for the respondents.

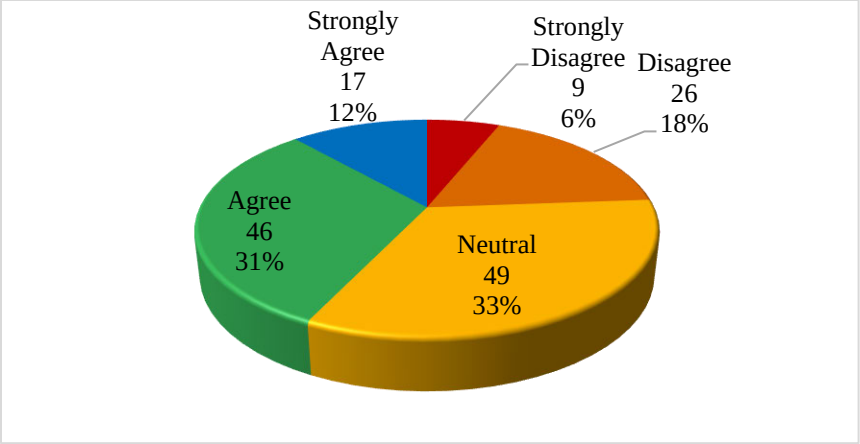

Figure 25. Respondents skill level

Table 9. below illustrates the full descriptive statistics performed on the responses for the figures in 4.6.1. In order to create the descriptive statistics, the responses were classified from "1", Strongly Disagree to "5", Strongly Agree.

The 95% confidence levels for the top three intentions were 0.14 for *monetary reasons*, 0.14 for *Fame and Prestige* and 0.13 for *Career advancement*. This indicated that with 95 % confidence, the population means for each of the above are *monetary reasons* with a population mean of between 4.02 (mean – confidence = 4.16 – 0.14 = 4.02) to 4.30 (mean + confidence = 4.16 + 0.14 = 4.30), leaning towards Agree, *Fame and Prestige* with population mean between 3.95 to 4.24, leaning towards Agree, and *Career advancement* with population mean between 3.76 to 4.02, leaning towards Agree. This indicated that the participants understood VDP's and their reason for participation.

The main reason individuals did not participate in VDP's was *Fear of punishment* with a 95% confidence level of 0.13 and a population mean of between 4.14 to 4.40, leaning towards Agree.

The top three motivators for individual to participate in VDP's were for *monetary reasons* to *earn an item/ gift* and *General software security*. The 95% confidence levels for these were 0.16 for *monetary reasons*

with a population mean between 3.94 to 4.26, leaning towards Agree, 0.16 to *earn an item/ gift* with a population mean between 3.80 to 4.12, leaning towards Agree and 0.14 for *General software security* with a population mean between 3.70 to 3.99, leaning towards Agree. This indicated that the participants required some reward in order to participate in VDP's.

The 95% confidence level for the skill level of the respondents was 0.17 and a population mean between 3.07 to 3.44, leaning towards Neutral. This indicated an average skill level regarding the ability to the discovery, exploitation and remediation of vulnerabilities.

	Monetary reasons	Fame or Prestige	Career advancement	Learn, the challenge or for the fun	Ethical Reasons	Malicious intent	Betterment of society	Fear of punishment	Legal concerns	Poor/ lack of VD platforms	Poor vendor communication	Monetary gain	To be on the Hall of Fame	To earn an item/ gift	General Software Security for all users	Hacking for fun	Malicious activities	Disclose it to the software vendor	Ignore a discovered vulnerability
Mean	4 16	4 10	3 89	3 89	3 65	1 80	3 55	4 27	3 99	3 48	3 61	4 10	3 68	3 96	3 84	1 83	1 48	4 18	1 80
Standard Error	0 07	0 07	0 07	0 07	0 07	0 09	0 08	0 07	0 07	0 08	0 08	0 08	0 09	0 08	0 07	0 11	0 09	0 07	0 09
Median	4	4	4	4	4	1	4	4	4	3	4	4	4	4	4	1	1	4	1
Mode	4	4	4	4	4	1	4	4	4	3	4	4	4	4	4	1	1	5	1
Standard Deviation	0 88	0 87	0 80	0 85	0 84	1 15	0 96	0 80	0 82	0 97	0 92	0 97	1 07	0 96	0 87	1 33	1 06	0 83	1 05
Sample Variance	0 78	0 76	0 65	0 73	0 71	1 32	0 92	0 63	0 67	0 95	0 86	0 94	1 14	0 93	0 76	1 77	1 11	0 69	1 11
Kurtosis	2 09	1 12	0 44	0 24	0 30	0 41	0 84	2 44	0 35	-0 78	-0 51	2 30	-0 21	0 75	0 48	0 01	3 69	-0 70	0 53
Skewness	-1 35	-1 07	-0 52	-0 59	-0 37	1 27	-0 74	-1 34	-0 58	0 03	-0 26	-1 48	-0 67	-0 99	-0 63	1 27	2 21	-0 58	1 13
Confidence Level (95 0%)	0 14	0 14	0 13	0 14	0 14	0 19	0 16	0 13	0 13	0 16	0 15	0 16	0 17	0 16	0 14	0 22	0 17	0 13	0 17

Table 9. Descriptive statistics of individuals intention to participate in VDP's

4.3.3.6 Benefits of organisations implementing VDP's

Figure 26. represents the responses in terms of the benefits organisations experience when implementing VDP's. The top three benefits were *Security benefits* with 141 (96%) of the responses, of which 72 (49%) responded with Agree and 69 (47%) with Strongly Agree, with a mean of 4.40, leaning towards Agree. This was followed by *Good governance* with 133 (91%) of the responses, of which 82 (56%) responded with Agree and 51 (35%) with Strongly Agree, with a mean of 4.23, leaning towards Agree. Lastly was *Raise awareness* with 124 (84%) responses, of which 85 (58%) responded with Agree and 39 (27%) with Strongly Agree with a mean of 4.07, leaning towards Agree. As per literature, VDP's provided security benefits as vulnerabilities are remediated, create a security community, and raise awareness, confirming the responses (Wysopal, 2002).

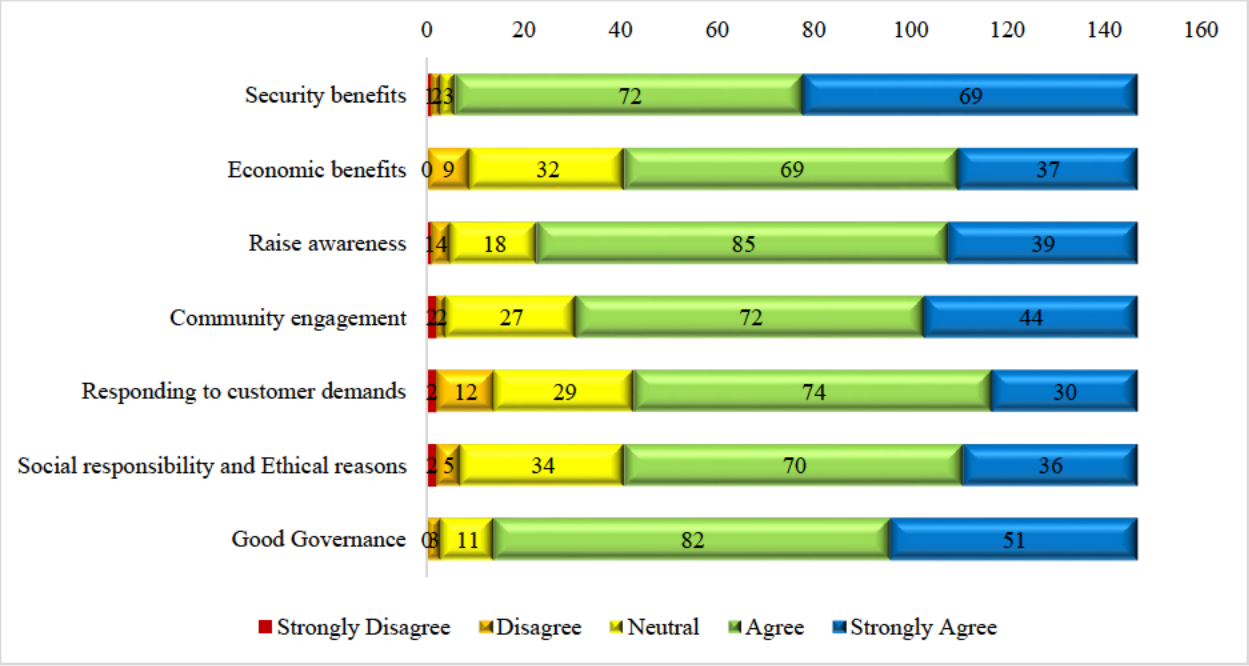

Figure 26. Organisational benefits of implementing VDP's

4.3.3.7 Organisations that have implemented VDP's

Figure 27. illustrates the number of respondent organisations that have a VDP policy. 31 (21%) mentioned that their organisation had a VDP policy, 116 (79%) mentioned that their organisations did not have a VDP

policy with 78 (53%) responding with Strongly Disagree, 16 (11%) with Disagree and 22 (15%) with Neutral. The overall mean was 2.10, leaning towards Disagree.

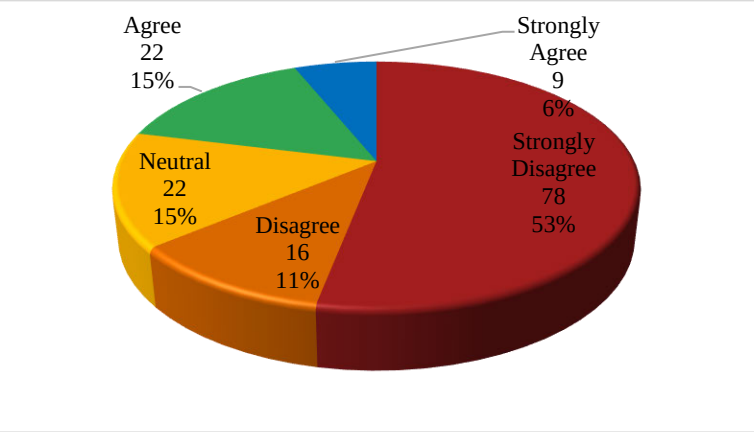

Figure 27. Organisation has a VDP policy

4.3.3.8 Organisational use of frameworks

Figure 28. highlights the number of respondent organisations that used or aligned with frameworks such as *ISO* and *COBIT*. 132 (90%) mentioned that their organisation used frameworks, 15 (10%) mentioned that their organisation did not use frameworks with 3 (2%) responding with Strongly Disagree and 12 (8%) with Neutral. The overall mean was 4.11, leaning towards Agree.

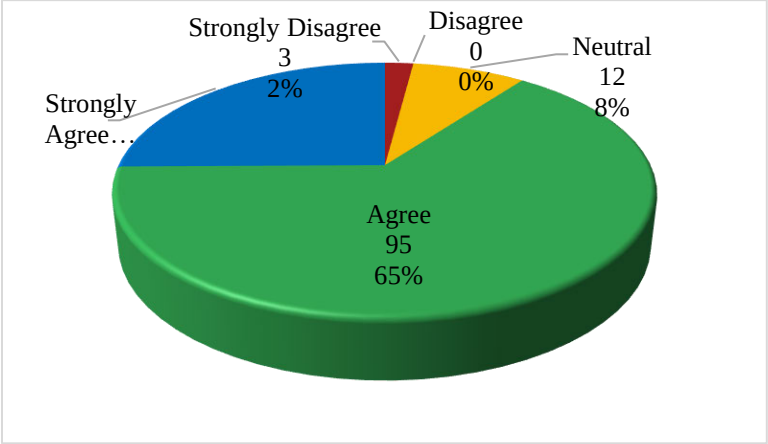

Figure 28. Organisational use of frameworks

4.3.3.9 Frameworks implemented at organisations

Figure 29. illustrates the types of frameworks used at the respondent's organisations. The top three frameworks used were *ISO Standards* with 130 (88%) of the responses. This was made up of 100 (68%) responding with Agree and 30 (20%) with Strongly Agree with a mean of 4.04, leaning towards Agree. This was followed by *COBIT* with 94 (64%) responding with Agree and 25 (17%) with Strongly Agree with a mean of 3.88, leaning towards Agree. Lastly, was *King IV*, with 85 (58%) responding with Agree and 27 (18%) with Strongly Agree with a mean of 3.85, leaning towards Agree. These frameworks as discussed in Chapter 2. had controls that related to VDP's.

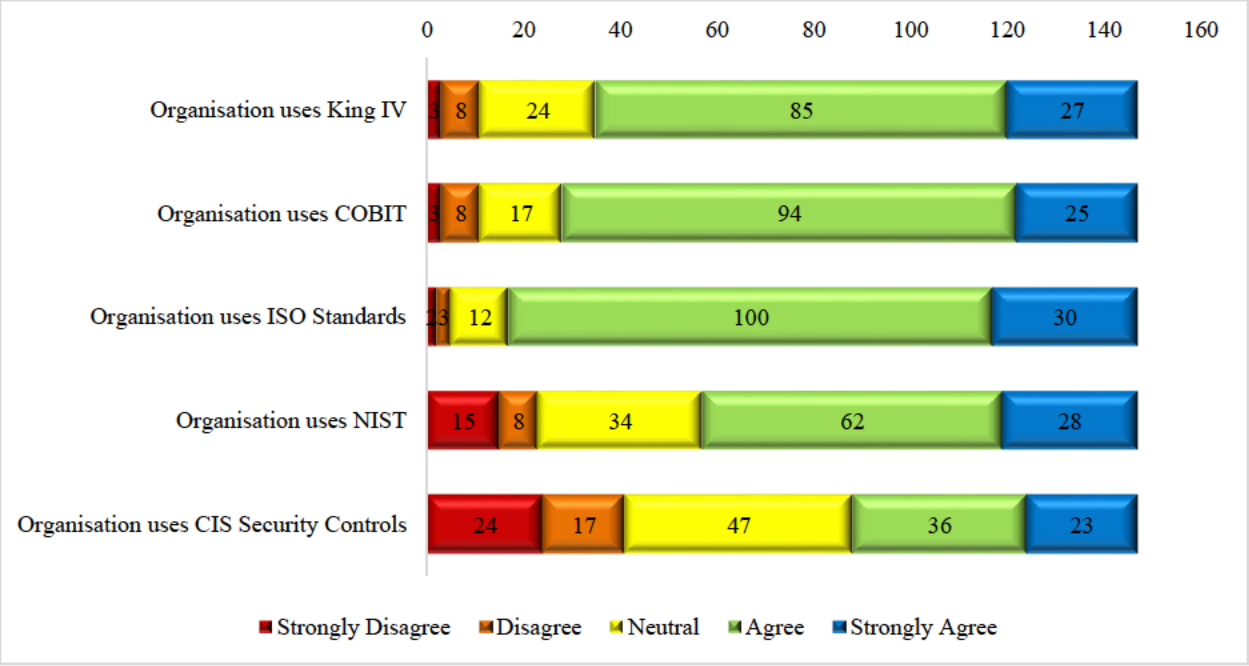

Figure 29. Frameworks implemented at organisations

In order to create the descriptive statistics, the responses were classified from "1", Strongly Disagree to "5", Strongly Agree. Table 10. illustrates the full descriptive statistics that were performed for the responses in 4.6.2.

	Security benefits	Economic benefits	Raise awareness	Community engagement	Responding to customer .	Social responsibility and Ethical reasons	Good Governance	Organisation has a Vulnerability Disclosure	Organisation follows ISO and COBIT.	Organisation uses King IV	Organisation uses COBIT	Organisation uses ISO Standards	Organisation uses NIST	Organisation uses CIS Security Controls
Mean	4.40	3.91	4.07	4.05	3.80	3.90	4.23	2.10	4.11	3.85	3.88	4.04	3.54	3.12
Standard Error	0.06	0.07	0.06	0.07	0.07	0.07	0.06	0.11	0.06	0.07	0.07	0.06	0.10	0.11
Median	4	4	4	4	4	4	4	1	4	4	4	4	4	3
Mode	4	4	4	4	4	4	4	1	4	4	4	4	4	3
Standard Deviation	0.67	0.84	0.75	0.81	0.90	0.85	0.67	1.35	0.71	0.85	0.82	0.70	1.17	1.28
Sample Variance	0.45	0.71	0.56	0.66	0.82	0.73	0.45	1.83	0.51	0.73	0.68	0.49	1.36	1.64
Kurtosis	4.88	-0.32	1.87	1.44	0.40	0.72	1.03	-0.83	5.81	1.63	2.48	4.69	0.05	-0.88
Skewness	-1.51	-0.46	-0.91	-0.86	-0.73	-0.68	-0.72	0.79	-1.54	-1.04	-1.27	-1.39	-0.83	-0.24
Confidence Level (95.0%)	0.11	0.14	0.12	0.13	0.15	0.14	0.11	0.22	0.12	0.14	0.13	0.11	0.19	0.21

Table 10. Descriptive statistics of organisations intention to participate in VDP's

The top three organisational benefits were *Security benefits, Good governance and Raise awareness* with a 95% confidence level of 0.11, 0.11 and 0.12 respectively. This indicated that with 95% confidence, the population means for each of the above were *Security benefits* with a population mean of between 4.29 (mean – confidence = 4.40 – 0.11 = 4.29) to 4.51 (mean + confidence = 4.40 + 0.11 = 4.51), leaning towards Strongly Agree, *Good governance* with population mean between 4.12 to 4.34, leaning towards Agree and *Raise awareness* with population mean between 3.95 to 4.19, leaning towards Agree. This indicated that participants understood what benefits organisations could have by implementing VDP's.

The 95% confidence level for organisations using frameworks such as *ISO and COBIT* was 0.12 with a population mean between 3.99 to 4.23, leaning towards Agree.

The top three frameworks used in organisations were *ISO Standards, COBIT and King IV* with a 95% confidence level of 0.11, 0.13 and 0.14 respectively. This indicated that with 95% confidence, the population means for each of the above were *ISO Standards* with a population mean of between 3.93 to 4.16, leaning towards Agree, *COBIT* with population mean between 3.75 to 4.02, leaning towards Neutral to Agree and *King IV* with population mean between 3.71 to 3.99, leaning to Neutral to Agree. This indicated that organisation have implemented governance frameworks.

4.3.3.10 Industry and Skills to discover, exploit and remediate vulnerabilities

Figure 30. illustrates the industry of the respondents with their skill level in terms of discovering, exploiting and remediating vulnerabilities. The top three industries with positive results were *Technology, Media and Communications* with 21(14%), followed by *Financial Services* with 13 (9%) and *Professional services* with 7 (5%). This indicates that *Technology, Media and Communications* has the largest skill set in terms of vulnerabilities with the remainder of industries lacking, likely due to poor awareness levels. This was

confirmed with the research findings by Lapena (2019), which stated that that their people and processes were the biggest challenge in terms of cybersecurity and vulnerability disclosure.

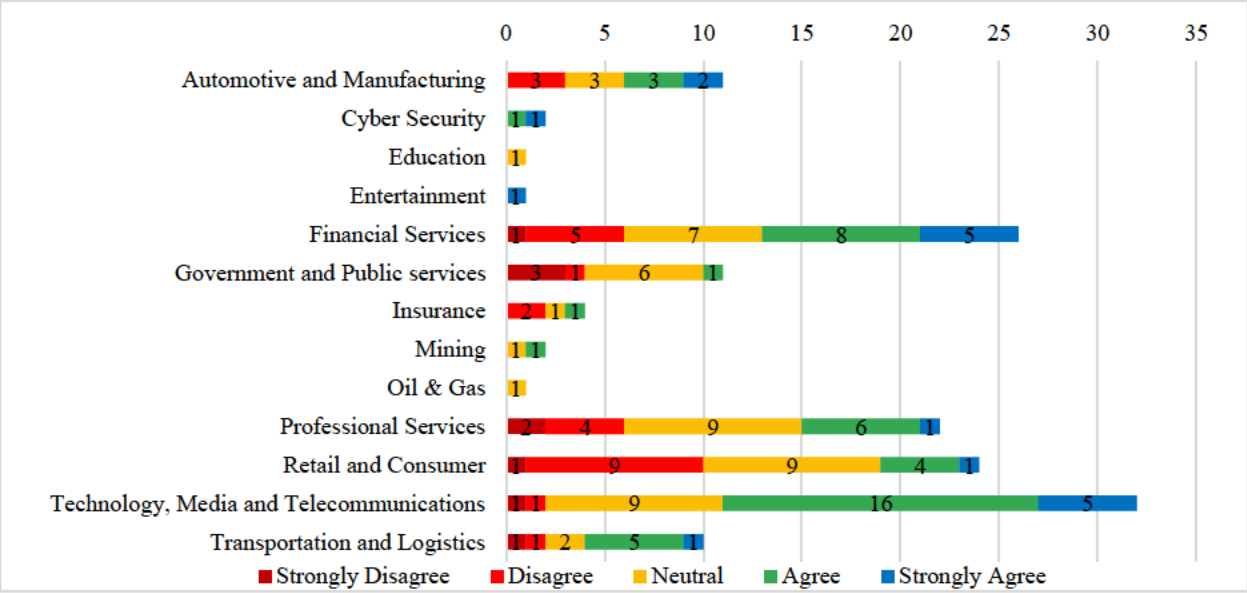

Figure 30. Industry and Skills to discover, exploit and remediate vulnerabilities

4.4 Correlations

This section delves into the correlations between the various questions in order to identify groups to validate the responses. Pearson Correlation Coefficient was used to perform the correlation as it measures the relationship between two continuous variables (Singh, 2006).

4.4.1 Correlation between the familiarity and understanding of VDP's

The correlation between the *familiarity of VDP's* and *understanding the processes associated with VDP's* as well as the *Types of VDP's* were calculated. The components that had two variables correlated are illustrated below in Table 11. The correlation matrix in Table 11, indicates a strong correlation (correlation coefficient, r, is greater than 0.5) between the F*amiliarity* and *Understanding of VDP's*. This could indicate that the respondents have a degree of awareness in relation to VDP's. It was also observed that

Understanding bug bounty programs has a weak correlation to familiarity and *Understanding of VDP's*. This could indicate that the respondents see bug bounty programs as separate programs and not associated with VDP's, as also indicated in the literature (Porup, 2018).

		Understanding of VDP's							
		Familiarity with VDP's	Understanding of VDP's	Understanding of the processes associated with VDP's	Understanding of Non-disclosure VDP's	Understanding of Self-disclosure VDP's	Understanding of Responsible-disclosure VDP's	Understanding of Full Disclosure VDP's	Understanding of Bug Bounty Programs
Familiarity with VDP's	Familiarity with VDP's	1.00							
	Understanding of VDP's	0.77	1.00						
	Understanding of the processes associated with VDP's	0.81	0.65	1.00					
	Understanding of Non-disclosure VDP's	0.58	0.44	0.67	1.00				
	Understanding of Self-disclosure VDP's	0.52	0.41	0.62	0.74	1.00			
	Understanding of Responsible-disclosure VDP's	0.56	0.42	0.62	0.63	0.70	1.00		
	Understanding of Full Disclosure VDP's	0.65	0.50	0.71	0.73	0.73	0.69	1.00	
	Understanding of Bug Bounty Programs	0.31	0.22	0.22	0.38	0.38	0.34	0.37	1.00

Table 11. Correlation between the familiarity and understanding of VDP's

4.4.2 Correlation between the organisational VDP policy and alignment to frameworks

The correlation between the *organisational VDP policy* and *alignment to frameworks* were calculated. The components that had two variables correlated are illustrated below in Table 12.

Alignment to Frameworks	Organisation has a Vulnerability Disclosure Program	Organisation follows ISO and COBIT.	Organisation uses King IV	Organisation uses COBIT	Organisation uses ISO Standards	Organisation uses NIST	Organisation uses CIS Security
Organisation has a Vulnerability Disclosure Program Policy	1.00						
Organisation follows ISO and COBIT.	0.23	1.00					
Organisation uses King IV	0.06	0.41	1.00				
Organisation uses COBIT	0.02	0.48	0.72	1.00			
Organisation uses ISO Standards	0.20	0.55	0.36	0.39	1.00		
Organisation uses NIST	0.31	0.26	0.09	0.10	0.44	1.00	
Organisation uses CIS Security Controls	0.47	0.18	0.03	0.11	0.25	0.63	1.00

Table 12. Correlation between organisational VDP policy and alignment to frameworks

The correlation matrix in Table 12, indicates a weak correlation (correlation coefficient, r, is greater than 0.5) between the *organisational VDP policy* and *alignment to frameworks*. This could indicate that the respondents and their organisations are not aware of the controls in these frameworks that address VDPs. It was also observed that *COBIT* has a strong correlation with *King IV*, indicating that respondents are familiar with governance frameworks and their implementation within the organisation. However, as per the response in Figure 4.23, majority of respondents mentioned that their organisations do not have a VDP policy showing misalignment to governance frameworks.

4.4.3 Correlation between Intention to Participate in VDP's and Action taken if a vulnerability is discovered

The correlation between a respondent's *intention to participate in VDP's* and the a*ction they would take if they discovered a vulnerability* was calculated. The components that had two variables correlated are illustrated below in Table 13.

Action taken if a vulnerability is discovered	Intention to participate in VDP's: Monetary reasons	Fame or Prestige	Career Advancement	Learn, the challenge or for the fun	Ethical Reasons	Malicious intent	Betterment of society
Disclose it to the software vendor	0.06	0.13	0.11	0.31	0.26	0.05	0.13
Ignore a discovered vulnerability	0.03	-0.11	-0.03	-0.02	-0.05	0.32	0.15
Keep a vulnerability secret and use it for malicious activities	0.01	-0.13	-0.06	0.02	0.07	0.54	0.24

Table 13. Correlation between Intention to Participate in VDP's and Action taken if a vulnerability is discovered

The correlation matrix in Table 13, indicates a strong correlation (correlation coefficient, r, is greater than 0.5) between a respondent's intention to not participate in VDP's for *Malicious Intent* and their action to *Keep a vulnerability secret and use it for malicious activities.* There was also moderate correlation (correlation coefficient, r, is between 0.3 to 0.5) between the respondent's intention to participate in VDP's to *Learn, the challenge or for the fun* and their action to *Disclose it to the software vendor.* This was in line with the responses whereby majority of the participants indicated that they would not participate in VDP's for malicious intent.

4.4.4 Correlation between Intention to Participate in VDP's and Motivation to discover vulnerabilities

The correlation between a respondent's intention to participate in VDP's and their motivation to discover vulnerabilities was calculated. The components that had two variables correlated are illustrated in Table 14.

Motivated to discover vulnerabilities	Intention to Participate in VDP's: Monetary reasons	Fame or Prestige	Career advancement	Learn, the challenge or for the fun	Ethical Reasons	Malicious intent	Betterment of society
Monetary gain	0.67	0.73	0.50	0.53	0.15	-0.18	0.02
To be on the Hall of Fame	0.53	0.48	0.41	0.36	0.15	-0.09	0.06
To earn an item/ gift	0.56	0.57	0.52	0.48	0.28	-0.24	0.10
General Software Security for all users	-0.07	0.04	0.23	0.41	0.51	0.10	0.31
Hacking for fun	-0.21	-0.15	-0.10	0.11	-0.01	0.56	0.23
Malicious activities	-0.10	-0.16	-0.05	0.07	0.08	0.65	0.23

Table 14. Correlation between Intention to Participate in VDP's and Motivation to discover vulnerabilities

The correlation matrix in Table 14, indicates a strong correlation (correlation coefficient, r, is greater than 0.5) between a respondent's intention to participate in VDP's for *Monetary Reasons* and *General Software Security for all users* and their motivation to discover vulnerabilities for *Monetary Gain, Fame or Prestige, Career Advancement and Learn, the challenge and for fun.* This supports literature that respondent's need some form of reward for participation in VDP's (Porup, 2018).

4.5 Reliability

The questions in table 13. below list the sections of the questionnaire where the Cronbach Alpha coefficient could be determined. The internal consistency is considered good when the Cronbach Alpha coefficient is between 0.8 and 0.9. The internal consistency is considered excellent where the Cronbach Alpha is greater

than 0.9. The internal consistency ranges from acceptable to excellent. Based on the results, it can de concluded that the study is reliable.

Questionnaire Section	Cronbach Alpha	Description
Section 2 - Overview	0.89670461	Internal consistency is good.
Section 3 – Challenges of VDP's	0.529280993	Internal consistency is acceptable.
Section 4 - Benefits of VDP's	0.869864149	Internal consistency is good.
Section 5.1 – Individual participation in VDP's	0.830093231	Internal consistency is good.
Section 5.2 - Organisational participation in VDP's	0.816896787	Internal consistency is good.

Table 15. Cronbach Alpha Coefficient

4.6 Key Findings

This research tried to answer the question on whether VDP's should be implemented as part of a cybersecurity strategy. This question was divided into three research objectives. Table 16. provides a summary of the key findings associated with each research objective.

No.	Research Objective	Findings
1.	To determine the challenges associated with vulnerability disclosure programs	• 58% of the respondent's understanding of the processes associated with VDP's fell into the Neutral, Disagree and Strongly Disagree categories, indicating a lack of familiarity and understanding of VDP's and the associated processes. • Not all VDP types were familiar amongst the respondents with Bug Bounty Programs being the most familiar with 82% of the responses. • 79% of the respondents stated that their organisations did not have a channel to report vulnerabilities. • The top three restrictions in implementing VDP's were lack of understanding of VDP's (91%), lack of management support (88%) and a lack of technical resources (78%). • 59% of the respondents also felt that the appropriate timeframe for a vendor to fix a vulnerability was > 30 days < 60 days. • 23% of the responses received from the IT Audit field in relation to their level of familiarity with VDP's, were negative.

No.	Research Objective	Findings
		• Based on the responses, very few South African companies have implemented VDP's. Technology, Media and Communications is a leader in terms of VDP implementation with (10% positive responses, this was followed by Financial Services with 3% and Retail and Consumer with 2%. • Very few South African companies have implemented a channel for reporting vulnerabilities. Technology, Media and Communications is a leader in terms of a reporting channel with 11% positive responses, this was followed by Financial Services with 6% and Retail and Consumer with 1%. • Technology, Media and Telecommunications has been made target of extortion with 8% of the responses.
2.	To determine the benefits associated with vulnerability disclosure programs.	• The top three benefits of implementing VDP's were improved security posture with 93% of the responses, reduces risk with 91% of the responses and increases cybersecurity awareness with 84% of the responses. • Majority of the respondents felt that VDP's should be a part of a cybersecurity strategy with 21% responses from Technology, Media and Telecommunications, followed by Financial services 17% and Retail and Consumer with 14%.

No.	Research Objective	Findings
3.	To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy.	• The top three intentions to participate in VDP's were monetary reasons with 50% of the responses, fame and prestige with 50% of the responses and career advancement with 50% of the responses. • 86% of the respondents did not feel that an individual's intent to participate in VDP's was malicious. • Majority (90%) of the respondents stated that individuals do not participate in VDP's out of fear of punishment, followed by legal concerns (47%) and poor vendor communication (40%). • The top three motivators to participate in VDP's were monetary reasons with 49%, to earn an item/ gift with 46% and general software security with 47%. • 80% of the respondents did not feel that individuals participate in VDP's for hacking for fun. • 78% of the respondents stated that they would disclose a vulnerability to the software vendor and 95% stated that they would not ignore a vulnerability. • 57% of the respondents stated that they did not have the necessary skills to discover, exploit and/or remediate vulnerabilities. • Organisations were noted to participate in VDP's for security benefits with 96% of the responses, good governance with 91% of the responses and to raise awareness with 84% of the responses. • 79% of the respondents stated that their organisations do not have a VDP policy. • 90% of the respondents stated that their organisations use frameworks such as ISO and COBIT.

No.	Research Objective	Findings
		• The top three frameworks used were ISO Standards with 88% of the responses, COBIT with 64% of the responses and King IV with 58% of the responses. • Technology, Media and Communications has the largest skill set in terms of vulnerabilities with 14% of the responses.

Table 16. Summary of findings per an objective

4.7 Conclusion

This chapter analysed and presented that results of the online questionnaire. The Cronbach's Alpha coefficient was calculated in order to determine the reliability of the study. The data was illustrated in two parts, the first part showing the demographics of the participants and the second part illustrating the findings aligned to each objective. The discussion on the findings were framed by the prior literature covered in chapter 2 with the findings being verified with literature. The chapter concluded with the analysis being summarised to illustrate the key findings per an objective as per Table 16. Conclusions based on the findings discussed in this chapter can now be drawn. The next chapter will discuss the conclusions, limitations of the study along with recommendations for future research.

CHAPTER FIVE – CONCLUSION, RECOMMENDATIONS AND LIMITATIONS

5.1 Introduction

This chapter provides a conclusion to the study and determines whether the research objectives were met. This research comprised of 5 chapters, including this chapter. Chapter 1 described the study and research approach. Chapter 2 discussed literature in terms of VDP's. Chapter 3 described the research design and methodology that guided this study. Chapter 4 analysed, presented and discussed the data that was collected. The data collected from the online questionnaire which was linked to the research objectives was intended to determine the challenges and benefits of VDP's and whether VDP's should be implemented as part of a cybersecurity strategy. This chapter will provide recommendations and opportunities for future research as well as the limitations of this research.

5.2 Research Findings and Conclusion

The objectives of the research were met and are discussed below. The main purpose of this study was to determine whether VDP's should be implemented as part of a cybersecurity strategy. The conclusions that follow were based on the results of the statistical analysis of the quantitative data.

5.2.1 Research Objective 1: To determine the challenges associated with vulnerability disclosure programs

The study established that the top three restrictions in implementing VDP's were a lack of understanding, lack of management support and lack of technical resources. These were required for a successful implementation. Section 4.3.1.1. discussed the familiarity and understanding of VDP's. Majority of the respondents were familiar with VDP's, but they lacked the understanding of the processes associated with VDP's as well as the different types of VDP's (Section 4.3.1.2.). Bug bounty programs were the most

familiar amongst respondents, indicating that they did not associate bug bounty programs as a type of VDP. Furthermore, responses received from the IT Audit space were negative in term of familiarity of VDP's. This indicated a clear lack of awareness of VDP's and the associated processes and types. Majority of the respondents indicated that their organisations did not have a channel to report VDP's. This was supported by the responses that very few South African companies have implemented VDP's when compared to Industry. The Technology, Media and Communications industry had majority of the responses for implementing a VDP and having a channel to report vulnerabilities. This again indicated the lack of awareness of VDP's across industries. It was evident from the responses that the Technology, Media and Communications industry was a victim of an extortion scheme due to a discovered vulnerability, possibly indicating their need to create a VDP (Section 4.3.1.3.). Industries such as the Financial industry and Retail and Consumer, also experienced extortion incidents and had implemented VDP's but the responses were minimal in comparison to Technology, Media and Communications. Other industries may not have disclosed such information possibly due to confidentiality clauses. As shown in Figure 2. of the adapted TBP model, the findings from the analysis indicates that the attitude towards vulnerability disclosure, vulnerability management and the knowledge of VDP policies, processes and technology affected the understanding of VDP's and the challenges experienced. This affected the action taken. This further indicated that in order to safeguard organisations from cyber-attacks, VDP's should be implemented to discover vulnerabilities early. The responses clearly indicated that apart from the identified restrictions in the implementation of VDP's as mentioned above, a lack of awareness is the greatest challenge associated with VDP's across industries and job roles.

5.2.2 Research Objective 2: To determine the benefits associated with vulnerability disclosure programs

The study found that the top three benefits of implementing VDP's were improved security posture, reduces risk and increases cybersecurity awareness. Majority of the respondents felt that VDP's should

be a part of a cybersecurity strategy (Section 4.3.2.2.) with most of the responses from Technology, Media and Telecommunications, Financial Services and Retail and Consumer (Section 4.3.2.3.). This supports the responses discussed in 5.2.1 whereby these three industries have implemented VDP's and had a channel to report vulnerabilities. The study confirmed that in South Africa, across industries, the benefits associated with VDP's was understood and the need for VDP's was recognised. As shown in Figure 2. of the adapted TBP model, the findings from the analysis indicated that the attitude towards vulnerability disclosure, vulnerability management and the knowledge of VDP policies, processes and technology affected the understanding of VDP's and the associated benefits experienced. This affected the action taken.

5.2.3 Research Objective 3: To determine whether a vulnerability disclosure program should be implemented as part of an overall cybersecurity strategy

The study determined that the top three intentions for individuals to participate in VDP's were monetary reasons, fame and prestige and career advancement (Section 4.3.3.1). This was motivated by monetary reasons, to earn an item or gift or general software security (Section 4.3.3.3). This confirmed that individuals require some type of reward in order to participate in VDP's. Majority of the respondents indicated that they would not participate in VDP's for hacking for fun or malicious activities (Section 4.3.3.2). They also indicated that if they were to discover a vulnerability that they would disclose it to the software vendor (Section 4.3.3.4.). These support their motivation of participating for general software security.

Majority of the respondents stated that they did not have the necessary skills to discover, exploit and/or remediate vulnerabilities (Section 4.3.3.5.). The top three industries with the necessary skills were Technology, Media and Communications, Financial Services and Professional services (Section 4.3.3.10.).

This supported the responses in 5.2.1 and 5.2.2, as these three industries have implemented VDP's, and saw the need for implementing VDP's as part of a cybersecurity strategy.

Organisational intention to participate in VDP's were security benefits, good governance and to raise awareness (Section 4.3.3.6.). This supported the individual's motivation to participate for the general software security. Good governance was associated with the responses received in terms of organisations having a VDP policy (Section 4.3.3.7.) and using frameworks such as ISO and COBIT. Majority of the respondents indicated that their organisations did not have a VDP policy (Section 4.3.3.8.) but used frameworks such as ISO and COBIT (Section 4.3.3.9.). It was also noted that the top three frameworks used were ISO Standards, COBIT and King IV. These three frameworks contain controls that were associated with VDP's. The responses showed a misalignment in terms of implementing VDP's and compliance to these frameworks. This can be linked back to 5.2.1.and the lack of awareness of VDP's.

The individual and organisational responses confirm that industries across South Africa have some knowledge of VDP's. In terms of framework compliance, organisations have implemented governance frameworks but have not implemented the controls associated with VDP's. For a VDP implementation to be successful, organisations should ensure that the policy is defined, processes created, and recognition and rewards established as these motivate individuals to participate. The reasons why individuals fear to participate in VDP's should also be explored and addressed in the implementation. As shown in Figure 2. Of the adapted TPB model, the findings from the analysis indicated that the skill level of individuals and the motivation to participate in VDP's affected the intended action to disclose a vulnerability, which affected their behaviour towards VDP's.

Based on the responses from 5.2.1, 5.2.2 and 5.2.3, it was determined that there was a need for VDP's to be implemented as part of a cybersecurity strategy. This would be driver of awareness and the overall implementation, which in turn would safeguard organisations against cyber-attacks. As per Figure 2. of the

TPB model, it would assist in changing the attitude of individuals and organisations, developing VDP policies and processes, upskilling peoples and implementing the appropriate motivators. In turn directing the intended action to disclose vulnerabilities, which changes behaviour. It would also assist in normalising vulnerability disclosure as it encourages proactive engagement with the security research community. A VDP as part of a cybersecurity strategy would ensure that the program is also measured according to the strategic key performance indicators, ensuring its success and compliance to frameworks.

5.3 Limitations

The questionnaire was only sent out to the ISACA SA community to understand their responses. There may have been a limitation with convenience sampling as other respondents outside ISACA could have responded but were not fully identified. Another limitation is that the respondents may have ignored or forgotten about the questionnaire that was emailed to them through ISACA SA, despite the numerous reminders and methods of distribution which resulted in the low response rate. Due to the method used, the researcher could not ascertain the reasons for this. It is possible that using hardcopy questionnaires or telephonic surveys may have assisted in obtaining a larger sample size as well as determine the reasons for non-response.

5.4 Recommendations

The research findings indicate that there is a need for VDP's, as across industry it was lacking. The proposed recommendations were based on the results of the study and literature.

5.4.1 Misalignment of controls from governance frameworks

It was determined from the discussion in 4.3.3 that there was a misalignment of the controls in governance frameworks such ISO, COBIT and King IV that impacted on the implementation of VDP's in organisations.

Controls in these frameworks should be reviewed to ensure compliance in terms of VDP's and their implementation thereof. It will assist organisations in determining the roles of each participant, definition of the processes to be followed for reporting and remediating vulnerabilities, determine the timeframes to remediate and publish a vulnerability as well as to determine the reward and/or recognition system. This will ensure a successful VDP implementation.

5.4.2 Awareness of VDP's

The responses in terms of familiarity, understanding of VDP's, the processes associated with VDP's and the types of VDP's indicate the lack of awareness. Organisations should spend time understanding the challenges, benefits of VDP's and the value of VDP's and educate their employees on its purpose.

5.4.3 Skills Gap

It was evident that there was a skills gap across the industries in term of discovering, exploiting and remediating VDP's. Individuals in the IT Auditing space require more training on VDP's especially if they are to act as consultants to support industry implementations of VDP's. Other industries should focus on upskilling staff in IT with the basics of vulnerability management in order to identify and report vulnerabilities.

5.4.4 Understanding Intention and Motivation for Participation

The study highlighted that respondents required some form of recognition or reward in order to feel motivated to participate in VDP's. Organisations planning on implementing VDP's should collaborate with security researchers and staff to understand what motivates them to participate in VDP's, in order to implement a successful VDP.

5.5 Opportunities for Future Research

The limitations determined during this study were used as guidance for future work. The following are recommended for future research on VDP's.

- The study revealed that organisations have limited understanding of VDP's in relation to the various governance frameworks. This resulted in misalignment of controls and non-compliance to governance frameworks. Future studies should be focused on the reasons for the limited understanding and corrective recommendations.
- More research is required on the different types of VDP's and how they can be implemented in organisations in accordance to frameworks.
- Future research should be extended across industries and not limited to the members of one organisation or location.
- Studies should consider using other sampling methods such as probability sampling for generalisability of the responses to the entire population.
- Repeat studies should be conducted to assess the growth of VDP's in South Africa.

5.6 Conclusion

This research explored the challenges, benefits of implementing VDP's. It analysed the reasons why individuals and organisations tend to participate and not participate in VDP's. This study contributed to the current knowledge base of literature in terms of VDP's and its associated processes. This chapter has focused on the objectives and research questions and drew conclusions thereof. It has outlined the areas where future research can be performed, which will provide more insight into VDP's. The major finding identified in this study was a general lack of awareness of VDP's, VDP types and the associated processes. Ultimately, this study demonstrated a step forward to understanding the challenges, benefits and whether VDP's should be implemented as part of a cybersecurity strategy. More understanding around the types of VDP's and frameworks that support VDP's would allow organisations to better implement VDP's. The

limitations highlighted in this chapter should be considered by future researchers of studies related to VDP's. The research objectives of this study have been met.

REFERENCES

Algarni, M. A., & Malaiya, K. Y. (2013). Most Successful Vulnerability Discoveres:Motivation and Methods. Colorado State, USA.

Barker, I. (2015). *organizations-take-too-long-to-fix-security-vulnerabilities*. Retrieved from betanews: https://betanews.com/2015/06/02/organizations-take-too-long-to-fix-security-vulnerabilities/

Barril Group. (2019, September 23). *Responsible Disclosure*. Retrieved from Barril Group: https://barril.co.za/pages/responsible-disclosure-1

Ben-Avie, J. (2017, October 3). *Vulnerability disclosure should be part of new EU Cybersecurity Strategy*. Retrieved from Mozilla: https://blog.mozilla.org/netpolicy/2017/10/03/vulnerability-disclosure-should-be-in-new-eu-cybersecurity-strategy/

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices.* Florida.

Bidorbuy. (2016, August 5). *Security Vulnerability Reporting Policy*. Retrieved from Bidorbuy: https://www.bidorbuy.co.za/help/6743/Security_Vulnerability_Reporting_Policy

Boston University. (2019, February). *Behavioral Change Models*. Retrieved from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories3.html

Bugcrowd. (2018). *2018 State of Bug Bounty.*

BusinessTech. (2013, August 22). *Joburg Billing Leak not a hack: Whistle Blower*. Retrieved from https://businesstech.co.za/news/government/44593/joburg-billing-leak-not-a-hack-whistle-blower/

Cencini, A., Yu, K., & Chan , T. (2005, December 2005). Software Vulnerabilities: Full, Responsible and Non-Disclosure. Washington.

Chandarman, R., & van Niekerk, B. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational. *AJIC Issue 20*, 133-155.

CIO. (2019, January 16). *What is COBIT? A framework for alignment and governance*. Retrieved from CIO: https://www.cio.com/article/3243684/what-is-cobit-a-framework-for-alignment-and-governance.html

Cisco. (2019, February 13). *What Is Cybersecurity*. Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cisecurity. (2019, February 14). *Incident Response and Management*. Retrieved from Cisecurity: https://www.cisecurity.org/controls/incident-response-and-management/

Delak, B. (2015). How to Evaluate Knowledge and Knowledge Management in the Organization Using COBIT 5. *Isaca Journal*, 1-5.

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. *Inf Syst Front*, 721-734.

Frost & Sullivan. (2018). *Analysis of the Global Public Vulnerability Research Market, 2017.* February.

Fruhlinger, J. (2017, October 17). *Petya Ransomware and NotPetya Malware: What You Need to Know Now*. Retrieved from CSOOnline: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

Gayomali, C. (2014, February 24). *Why Do Companies Keep Getting Hacked?* Retrieved from Fastcompany: https://www.fastcompany.com/3026672/why-do-companies-keep-getting-hacked

Graz University of Technology. (2018). *Meltdown and Spectre*. Retrieved from Meltdownattack: https://meltdownattack.com/

Hackerone. (2019, September). *About Hackerone*. Retrieved from Hackerone: https://www.hackerone.com/about

Hackerone. (2019, September). *MTN*. Retrieved from Hackerone: https://hackerone.com/mtnloaded

Intel. (2019, September). *Intel Bug Bounty Program*. Retrieved from Intel: https://www.intel.com/content/www/us/en/security-center/bug-bounty-program.html
International Organization for Standardisation. (2013). ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management. New York.
International Organization for Standardisation. (2013, November). *ISO/IEC 30111:2013*. Retrieved from ISO: https://www.iso.org/standard/53231.html
International Organization for Standardisation. (2018, October). *ISO/IEC 29147:2018*. Retrieved from ISO: org/standard/72311.html
IOL. (2018, June 21). *South Africans losing R2.2 billion a year to cyber attacks*. Retrieved from IOL: https://www.iol.co.za/capeargus/news/south-africans-losing-r22-billion-a-year-to-cyber-attacks-15601682
ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Illinois, USA.
ISO. (2018). *ISO/IEC 29147:2018(en)*. Retrieved from ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en
JPMorgan Chase & Co. (2019, September). *Responsible Disclosure*. Retrieved from JPMorgan Chase & Co: https://responsibledisclosure.jpmorganchase.com/hc/en-us
Kothari, C. R. (2004). *Research Methodology Methods and Techniques.* Jaipur: New Age International Publishers.
KPMG South Africa. (2016). King IV Summary Guide. South Africa.
Kranenbarg, M. W., Holt, T. J., & van der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime ScienceAn Interdisciplinary Journal 2018*.
Lapena, R. (2019, June 3). *Unpatched Vulnerabilities Caused Breaches in 27% of Orgs, Finds Study*. Retrieved from Tripwire: https://www.tripwire.com/state-of-security/vulnerability-management/unpatched-vulnerabilities-breaches/
Miller, J. (2019, April 30). *DHS Tells Agencies to Move Faster to Fix Critical Cyber Vulnerabilities*. Retrieved from Federalnewsnetwork: https://federalnewsnetwork.com/cybersecurity/2019/04/dhs-tells-agencies-to-move-faster-to-fix-critical-cyber-vulnerabilities/
Mimecast. (2019, August). *Mimecast's Responsible Disclosure Policy*. Retrieved from Mimecast: https://www.mimecast.com/responsible-disclosure/
MultiChoice. (2019, September 27). *MultiChoice Responsible Disclosure Policy*. Retrieved from MultiChoice: https://www.dstv.co.za/legal/multichoice-responsible-disclosure-policy/
National Cyber Security Centre. (2018). *Policy for Arriving at a Practice for Responsible Disclosure.* Retrieved from media2.mofo.com: https://media2.mofo.com/documents/responsible-disclosure-eng.pdf
National Telecommunications and Information Administration. (2015). *Vulnerability Disclosure Attitudes and Actions.* National Telecommunications and Information Administration.
Nike. (2019, September). *What is Nike's Responsible Disclosure Program?* Retrieved from Nike: https://www.nike.com/help/a/responsible-disclosure
NIST. (2017, June). *About NIST*. Retrieved from NIST: https://www.nist.gov/about-nist
NVD. (2019, February 13). *NIST Special Publication 800-53 (Rev. 4)*. Retrieved from NATIONAL VULNERABILITY DATABASE: https://nvd.nist.gov/800-53/Rev4/control/AC-21
Ponemon Institute LLC. (2019). *Costs and Consequences of Gaps in Vulnerability Response.* Ponemon Institute LLC.
Porup, J. M. (2018, August 7). *Do You Need a Vulnerability Disclosure Program? The Feds Say Yes*. Retrieved from Csoonline: https://www.csoonline.com/article/3294418/vulnerabilities/do-you-need-a-vulnerability-disclosure-program-the-feds-say-yes.html
Porup, J. M. (2018, May 14). *Katie Moussouris: It's dangerous to conflate bug bounties and vulnerability disclosure*. Retrieved from csoonline: https://www.csoonline.com/article/3271088/katie-moussouris-its-dangerous-to-conflate-bug-bounties-and-vulnerability-disclosure.html
Pubal, J. (2017, December). Bug Bounty Programs.

Pupillo, L. (2017, July 31). *Software Vulnerabilities Disclosure: The European landscape*. Retrieved from CEPS: https://www.ceps.eu/publications/software-vulnerabilities-disclosure-european-landscape
PwC. (2018). *Global Economic Crime and Fraud Survey 2018: 6th South African Edition.* PwC.
PwC. (2019). *22nd Annual CEO survey*. Retrieved from PwC: https://www.pwc.co.za/en/press-room/22nd-annual-ceo-survey.html
PwC. (2019). *22nd Annual Global CEO Survey*. PwC.
Rapid7. (2019). *Vulnerabilities-exploits-threats*. Retrieved from Rapid7: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/
Rauniar, R., Rawski, G., Yang, J., & Johnson, B. (2014). Technology Acceptance Model (TAM) and social media usage: an emperical study on Facebook. *Journal of Enterprise Information Management, Vol.27 Iss 1*, 6-30.
Rhodes-Ousley, M. (2013). *The complete reference information security second edition.* New York: Mcgraw-Hill companies.
Rouse, M. (2018, August 31). *WannaCry Ransomware*. Retrieved from Searchsecurity.com: https://searchsecurity.techtarget.com/definition/WannaCry-ransomware
Ruohonen, J., & Allodi, L. (2018). A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities. *arXiv:1805.0985v1*.
Sass, R. (2019, January). *Software Vulnerabilities Are on the Rise — Here's why*. Retrieved from ITproportal.
Searchsecurity. (2019, February 14). *Vulnerability Disclosure*. Retrieved from Searchsecurity.com: https://searchsecurity.techtarget.com/definition/vulnerability-disclosure
Sekaran, U., & Bougie, R. (2010). *Research methods for business: A Skill building Approach. 5th Edition.* United Kingdom: John Wiley and Sons.
Sekaran, U., & Bougie, R. (2013). *Research Methods for Business.* UK: John Wiley & Sons Ltd.
Singh, Y. K. (2006). *Fundamental of Research Methodology and Statistics.* Chitrakoot: New Age International Publishers.
TechTarget. (2019, February). *Vulnerability (Information (Technology)*. Retrieved from TechTarget: https://whatis.techtarget.com/definition/vulnerability
Thompson, D., & Trilling, S. (2018, November 28). *Cyber Security Predictions: 2019 and Beyond*. Retrieved from https://www.symantec.com: https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond
Trochim, W. M. (2020, January 6). *Sampling*. Retrieved from Social Research Methods: https://socialresearchmethods.net/kb/sampling.php
US DOJ. (2017, July). A Framework for a Vulnerability Disclosure Program for Online Systems. Washington, USA.
Vidstrom, A. (2002, April 8). *Full Disclosure of Vulnerabilities – pros/cons and fake arguments.* Retrieved from Helpnet: https://www.helpnetsecurity.com/2002/04/08/full-disclosure-of-vulnerabilities---proscons-and-fake-arguments/
Williams, D. M., Rana, P. N., & Dwivedi, K. Y. (2015). The Unified Theory of Acceptance and Use of Technology (UTAUT): A Literature Review. *Journal of Enterprise Information Management, 28(3)*, 443-488.
Williams, J. (2016, September). *Uploads.* Retrieved from Isaca: https://www.isaca-events.org.za/wp-content/uploads/2016/09/justin-williams_friend-or-foe_community-engagement.pdf
Wysopal, C. (2002, February). Responsible Vulnerability Disclosure Process. Internet Engineering Task Force.

APPENDIX: ETHICAL CLEARANCE

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

14 August 2019

Ms Trishee Jobraj (200100522)
School Of Man Info Tech & Gov
Westville Campus

Dear Ms Trishee Jobraj,

Protocol reference number: HSSREC/00000075/2019
Project title: The role of vulnerability disclosure programs in an organisational cybersecurity strategy

Full Approval – Expedited Application

This letter serves to notify you that your application received on 21 July 2019 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

This approval is valid for one year from 14 August 2019.
To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

Yours sincerely,

[redacted]

Professor Urmilla Bob
University Dean of Research

/dd