CYBERCRIME AWARENESS AND REPORTING IN THE PUBLIC SECTOR IN BOTSWANA

A DISSERTATION PRESENTED TO THE

Department of Information Systems

University of Cape Town

By

Sinka Matengu – MTNSIN004

NOVEMBER 2012

In partial fulfilment of the requirements for

MASTERS OF COMMERCE

(INFORMATION SYSTEMS)

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this report from the work(s) of other people has been attributed, and has been cited and referenced.
3. This thesis is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

_____ _____

Sinka Matengu Signature: Date:

(MTNSIN004)

Acknowledgements

I would like to thank the following people for their valuable assistance and direction in completing this study:

- My supervisor, Adrie Stander for mentoring, guiding and always having faith in me.
- Professor Mike Hart for providing expert guidance with the statistical analysis.
- Professor Mike Kyobe for the assistance and guidance for IS theories and data analysis.
- My Course Coordinator (Class of 2011), Professor Irwin Brown for the useful material and insightful guidance during the course of study.
- Freda Parker for the valuable administration assistance during the course of study.
- The Government of Botswana for the opportunity it afforded to me to further my studies.
- The participants for their valuable time used to complete the questionnaires in order to provide the necessary data for this research.

Dedication

I dedicate this thesis to my wife Agnes Matengu-Sinka, my son Muheewa Samuel Matengu-Sinka, my grandmother Vana Nãndu, my mom and dad, my sisters, my in-laws, my nephews, my niece and all my friends for their love, invaluable support and encouragement throughout the period that I spent working on this research.

Lastly, I would also like to dedicate this dissertation to the memories of my beloved late brother and friend Mubita Victor Matengu (Sha Ronnie), and also to my father-in-law and friend Duncan D. Mlazie (D.D.) for the support and encouragement they gave to me during the challenging early days of my studies.

Abstract

Information and Communication Technologies (ICTs) have been widely adopted by both profit making and non- profit making organisations around the world in the 21st century, in order to exploit the envisaged benefits that are associated with ICTs. These benefits include improved productivity, better efficiency, cost reductions, better quality of services and products, timely delivery of services, increased profits and many others. As a result governments in developed and developing nations around the world have also invested in ICT in order to improve service delivery to their citizens and clients, among other reasons. With time ICTs have improved and expanded to offer better services, such as increased bandwidth and more affordable Internet connectivity. Therefore, this has resulted in an attractive environment for cybercrime. Unfortunately for most developing countries especially in Africa, this is a serious challenge since they currently lack necessary controls and effective cybercrime legislation to secure their infrastructure.

Different authors have reported on the problem of cybercrime and other concepts that are associated with it. The studies looking at the area of ICT and cybercrime are examined and assessed to identify gaps that exist. Nevertheless, most of these studies focused more on developed countries, and did not emphasise on the public sector. Therefore, their findings might not be appropriately applicable to governments in developing countries especially within the Africa context.

This study seeks to investigate factors that are necessary to enable the Botswana public sector to properly report on cybercrime attacks. The ICT environment of Botswana government is explored to determine the extent of ICT utilisation in the public sector. Based on the literature survey, a research framework for reporting cybercrime for the Botswana public sector is formulated.

To carry out the study the research adopted a quantitate approach with a positivistic viewpoint. It used a hardcopy paper questionnaire that was administered to Botswana public employees who formed its sample in the capital city of Gaborone. The collected data was statistically tested in

order to provide empirical validation for the research framework with the Botswana public sector.

Findings for this research showed that Cybercrime Awareness, User Training on Information Security Awareness, and Understanding of Cybercrime Legislation significantly impact on the ability of users to report on cybercrime attacks within the Botswana public sector. Furthermore, it was established that Organisational Culture and User Training on Cybercrime Awareness have a significant impact on Cybercrime Awareness within the Botswana public sector.

The study also outlines the nature of significance of these results to the academic world and also for practical purposes within the Botswana public sector. Lastly areas for future research are outlined.

Table of Contents

Table of Figures

List of Tables

List of Acronyms

BBS	-	Bulletin Board System
BTC	-	Botswana Telecommunications Corporation
CoE	-	Council of Europe
CSI	-	Computer Security Institute
DDoS	-	Dedicated Denial of Service
DIT	-	Department of Information Technology
DOS	-	Disk Operating System
EASSy	-	Eastern Africa Sub-marine Cable System
E-education	-	Electronic Education
E-government	-	Electronic Government
GDN	-	Government Digital Network
HR	-	Human Resources
IT	-	Information Technology
ICT	-	Information and Communication Technology
NGO	-	Non-Governmental Organisation
NHCTU	-	National High-Tech Crime Unit
OECD	-	Organisation for Economic Cooperation and Development
PDA	-	Personal Data Assistant
SOCA	-	Serious Organised Crime Agency
UK	-	United Kingdom
UN	-	United Nations
USA	-	United States of America
WACS	-	West African Cable System

Chapter 1 - Introduction

1.1 Background and Context

The government of Botswana has embraced the use of Information and Communication Technology (ICT) which is now wide spread in its different departments and public institutions around the country (Republic of Botswana, 2010). This move was precipitated by the presumed benefits such as cost efficiency, productivity, and better service delivery to the public which are being realised by the private sector which adopted the technology before government did (Kyobe, 2010; Moloi & Mutula, 2007). Furthermore other countries both in Africa and overseas also use ICT to deliver their services (Longe, Ngwa, Wada, Mbarika, & Kvasny, 2009; Morawczynski & Ngwenyama, 2007).

The increase in ICT adoption has resulted in problems such as cybercrime to also be realised in Botswana and other parts of Africa due to the fact that there are less or no controls to secure the infrastructure, leaving criminals to act as they please (Longe et al., 2009; Ochieng, 2011). This situation is further worsened by the fact that Botswana, like South Africa (Nyanda, 2010) does not yet have clear guidelines to help with the implementation of the new Cybercrime and Computer related Crime Act which was introduced in 2007 (Ngakaagae, 2010). Due to the above limitation the government or public sector may at times not even be aware of cybercrime attacks experienced, which make it hard to report or account for them at all.

1.2 Research Purpose

The main aim of this research is to investigate factors that hinder Botswana public sector organisations from recognising and reporting properly on cybercrime attacks.

The purpose of this research is to develop a framework that will enable the public sector in Botswana to recognise and report on cybercrime attacks. To achieve this, the research will investigate and identify factors that impact the public sector in Botswana to recognise and report on cybercrime attacks. Eventually an effective tool (framework) will be delivered that the public sector can utilize to address this problem.

1.3 Research Objectives

This research has the follows objectives which it aims to achieve:

1. To conduct a literature review on the issue of cybercrime and identify factors that impact the ability to report cybercrime attacks within an organisation.
2. To develop a research framework from literature that can enable the Botswana public sector to report cybercrime attacks.
3. To empirically validate the research framework within the context of the Botswana public sector using questionnaires.
4. To identify future research areas in relation to this study.

1.4 Research Scope

The focus of this study is to determine factors that impact on the ability to report cybercrime attacks in an organisation. Such knowledge could be used to educate ICT users on how to report incidents or attacks of cybercrime if they occur within an organisation. This covers general knowledge and concepts of cybercrime both in developed and developing countries, including Africa.

This research does not focus on a specific government department or ministry, but rather it aims to assess the overall atmosphere within the Botswana public sector as far as cybercrime is concerned. However, a deliberate decision was made to include certain units that are of interest to this study, namely: the Information Technology (IT) unit, Human Resources (HR) unit, heads of units or departments and senior management because of specific reasons that will be elaborated more in sections to follow. In general the study aims to include as many users of ICT from different government ministries as much as possible in order to build a sample that is representative of the Botswana government.

1.5 Research Value

The importance of this study is in twofold, both theoretically and practically. It will contribute to the field of Information Systems by providing insight into the developing world especially with an African perspective of dealing with cybercrime in the public sector, for

which there is currently limited literature. The work that has been done by academics on cybercrime on this sector mostly addresses the developed countries where ICTs have been in existence for a considerable number of years compared to Africa. Furthermore, there is a limitation in studies that investigate factors within the public sector that affect the management of cybercrime.

On a practical level the study will provide a framework that the Botswana government and maybe other similar African countries can use to raise the level of awareness for cybercrime and also reporting of incidents within the public sector. This will be very helpful given the fact that the Botswana government has started to implements its e-government initiative that when fully implemented will result in more information being available digitally, and most government services offered on-line to the public. Therefore, the framework developed by this study could be used to raise the level of awareness among employees within the public sector to enable them to better identify and report cybercrime attacks.

This study can also provide an opportunity for the Botswana government to develop clear guidelines on how to fight cybercrime and implement the Cybercrime and Computer Related Crimes Act of 2007, which most people do not yet understand or know since it has no clear guidelines (Ngakaagae, 2010). Such guidelines would also enable the law enforcement and legal departments within the government to manage cybercrime offenses better as stipulated by the Act. Finally, results from this study can be used to facilitate further studies for research in sectors other than the public sector to analyse whether the research framework applies to them or even to other African countries.

1.6 Dissertation Overview

The dissertation is presented in various chapters that have been broken down as follows: in the abstract, the summary of the purpose and scope of research, the chosen methodology as well as key findings and the conclusion are given.

Chapter 1: gives the introduction followed by the research background, the research purpose and objectives; finally it also highlights the importance of the research.

Chapter 2: presents the literature review on the area of cybercrime and other related concepts to provide an understanding for the research area. This information is used to later formulate the research framework that was tested imperially for this study. This chapter ends by presenting identified gaps in the literature in order to motivate this study.

Chapter 3: contains the research framework to be used in this study. It also provides a thorough explanation to the research model, research questions and refined objectives. The research hypotheses used to test the framework are also provided.

Chapter 4: presents the research methodology used in the study. Areas that are covered include underlying philosophy, sample plan; methods used for data collection, techniques for data analysis, the research framework and relevant ethical considerations. Also the research design instruments are explained.

Chapter 5: gives all the descriptive analyses results obtained from the sample data. This includes descriptions for respondent profiles, questionnaire items and constructs.

Chapter 6: contains the different tests conducted during analysis for instrument validity and reliability.

Chapter 7: presents results obtained from hypotheses testing with the corresponding analysis and evaluations. Implications for findings are also given. The research summary findings and refined research framework are also provided. Lastly, the additional findings are discussed.

Chapter 8: is a conclusion for the dissertation; reviewing concepts presented in other sections. Then implications for the study findings are also given for academics and practitioners. It ends with future study recommendations and limitations for the study.

Chapter 2: Literature Review

This chapter provides findings obtained from other studies that analysed concepts and findings from cybercrime and related ICT issues.

2.1 What is Cybercrime?

The term cybercrime has been used by academics, IT professionals, business people and general computer users. Despite this, it does not have an agreed definition but is defined in various ways (Fafinski, 2007; Kshetri, 2010). There is also no statute or legal definition of cybercrime (Arpana & Chauhan, 2012). Nagpal (2008) defines it as any unlawful act where the computer is used as a tool, target or both. He goes on to say a computer can be any device such as a laptop, desktop, cell phone, smart watch or PDA (Personal Data Assistant). It is also referred to as any crime that involves a computer and a network, where a computer can be the target of the crime such as Denial of Service (DoS), virus and malware infections; the computer in other instances can also be used to commit a crime such as cyber stalking, fraud, identity theft, hacking and copyright infringements (Cardoso, 2007).

There is also another dimension of this crime where the computer is used as an accessory to hold stolen data or information (Sukhai, 2004). The Council of Europe convention uses the word to include offenses committed against data, its contents and copyright breaches (Archick, 2004). It is also considered to be fraud, forgery and unauthorised access (United Nations, 1995).

Cybercrimes can be classified into two classes: the first being crimes that involve a computer network attacking other networks, such as when malicious code or viruses are used to disable computer systems. The second one is where computer networks are used to attack targeted users; examples include fraud, copyright infringement, identity theft, intrusion and others that target individuals or organisations (Arpana & Chauhan, 2012).

This lack of an agreed definition leads to an unclear understanding of what cybercrime really is, and how to prevent and manage it (Fafinski, 2007; Gordon & Ford, 2006). This situation results in confusion for users to know what it or how to identify when such a crime has occurred or even know whether they are engaging in cybercrime offences themselves.

For this study the following definition shall be adopted as: "any crime that is facilitated or committed using a computer, network, or hardware device; the computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime" (Gordon & Ford, 2006, 14). This definition tries to be more encompassing and avoids limiting cybercrime to cover only illegal activities that individuals carry out while online (Rho, 2007).

2.2 History of Cybercrime

This section looks at the history of cybercrime to get an insight of how it evolved with time to be what it is today. This might shed light on some obscure issues regarding the crime.

Cybercrime started around the period of 1979 – 1983 with young boys (from USA, Europe, Australia and Canada) playing with home computers (based on DOS (Disk Operating System) and accessing the BBS (Bulletin Board System) to learn how to connect to the X.25 public data network system in order to find any open networks to connect to and satisfy their curiosity. Then from around 1986 – 1990s the upcoming underground hacking world developed their own magazines called '2600' and Hacker's Quarterly; through which they could share their skills and ideas. This enabled hackers in different countries to collaborate and hack as a group and then share their findings on the BBS. During this period the USA (United States of America) military and government computer systems were targeted; this was done for gaining recognition and enhancing skills (Chiesa, 2010).

During the period 1995 – 2000, when the Internet was introduced in a number of countries, the school hackers learnt how to use the X.25 public data network system to connect to the Internet and then explored their skills to hack into universities, government, and military systems in order to 'show off' to their friends. With the aid of the Internet the hackers started writing and distributing exploits or attack codes easily, and in 2000 Michael Calce retrieved DDoS (Distributed Denial of Service) codes from the internet which he later used to stop services on eBay, Amazon and Yahoo websites. This ushered in the new threat of what these inexperienced hackers could do to online businesses globally (Think Quest, 2011). At this point the organised crime groups like the Mafias in Europe realised the opportunity to make money through these exploits, and started hiring these programmers (coders) around the world to develop malicious code for them to exploit computer systems and make money through scams.

From the period 2001 – 2005 cybercrime officially became established with the introduction of well organised and planned attacks with financial motives. This was augmented by the fact that hackers and Mafia criminals collaborated together which resulted in easy availability of highly sophisticated malicious software and infrastructure and also that there was now a global proliferation of fast Internet connections which also introduced new services like e-commerce (electronic commerce). This made it easy for cybercrime to become global in nature (Think Quest, 2011).

From the years 2005 to date, cybercrime took a different turn with new players entering the scene to harness the power of the Internet to launch attacks that were not possible before. These included foreign governments and their militaries. The Chinese military in 2007 hacked into the US Defence Department's email system and took it down for over a week, however China denied the allegations. During the same year of 2007 the Israeli air defence is reported to have disabled the Syrian military air defence radar detection system for warplanes by taking advantage of an undisclosed "disable switch" found on the radar computer system's chip. This enabled the Israeli army jets to bomb a site suspected to be a nuclear reactor in Syria (Businessweek, 2012).

Still yet in 2007, businesses, churches, governments and NGOs became victims to the Zeus botnet where their networks were compromised. The attack was initiated through phishing techniques using an email to attract users to click on a link which installed malicious software on computers which would capture keystrokes to steal banking details. Investigations showed that about US$70 million was lost through Zeus and around 100 perpetrators worldwide were arrested. In 2008 during the US presidential elections, an attack on both Mr Obama and Mr McCain's computer network was reported by the FBI; this originated from a foreign government which was later identified as China. The purpose of the attack was to gather information regarding the two candidate's policy plans (Businessweek, 2012).

With the entrance of foreign governments in the cybercrime scene, the nature and purpose of attacks has been changed drastically. In January 2010 Google reported that it discovered a very sophisticated attack on its Gmail network for accounts of activists for human rights; the attacks originated from China. These attacks prompted Google to consider withdrawing its services from China. Still in the same year of 2010, a new worm called Stuxnet was

discovered in June. This worm targeted industrial computers systems installed with Siemens software that were also used in Iran where the worm was reported to have been highly detected. This lead to researchers speculating the possibility of the worm's origins to be either from the United States or Israel which was meant to sabotage Iran's nuclear ambitions (Businessweek, 2012).

The evolution of cybercrime which was characterised with underground activities made it difficult for people to understand what its true nature was; hence this resulted in little information being available in the public domain which accounted for why there was no clear agreement of what it was or how to manage it (Gordon & Ford, 2006).

2.3 Cybercrime Reporting

A continued rise in criminals' use of ICT to commit crime has been noticed over the past few years (Rustad, 2001); on the other hand challenges with cybercrime legislation, limitation for resources and skills by law enforcement agencies makes it hard for most crimes to be successfully addressed (Akuta et al, 2011). This has resulted in individuals and a number of organisations to fall victims to such crimes. Therefore to address this problem, organisations need to develop and or improve on their cybercrime reporting policies and strategies in order to address this situation (Computer Security Institute, 2011).

The following reasons have been pointed out in support of why cybercrime needs to be addressed:

- To develop initiatives that will reduce the cybercrime
- To enhance response from other stakeholders both locally and internationally
- To identify limitations within existing responses
- To aid in decision making and assessment of risks
- To develop cybercrime prevention measures
- To enable better cybercrime reporting
- To help in public education and awareness

(Fafinski, Dutton & Margetts, 2010).

Cybercrime reporting is already being addressed by organisations both in government and private sector, mostly in the USA; however there are challenges which still exist. One of

these is that there are a lot of organisations that are involved in the collection of cybercrime activities within different countries. Furthermore, these organisations and countries do not collaborate to share and consolidate their records. These organisations include the police, private companies, academic institutions, other government agencies and Non-Governmental Organisations (NGOs). This results in challenges for mapping the real extent of cybercrime (Fafinski et al., 2010).

Reporting challenges are also worsened by the fact that records which are held by the police are generally under-reported or even under-recorded in some instances due to a number of reasons. For example, the United Kingdom (UK) in 2001 established an agency, the National High-Tech Crime Unit (NHCTU) to handle cybercrime matters both nationally and across the border. This agency received substantial reports both from the public and business areas because it had a confidential clause to protect the reporters (Valerie et al., 2006).

However, a few years later, in order to consolidate reporting functions in UK, operations of three separate agencies were merged together; among them was NHCTU, to form the Serious Organised Crime Agency (SOCA) cybercrime reporting. SOCA removed the confidentiality clause for reporting by NHCTU; this move has been feared could result in few incidents being reported compared to before (Bennett, 2006).

Following the 2001 terrorist attacks in the USA, the federal government initiated a thorough review of its internet security policies. This resulted in the assignment of cyber national security to the Department of Homeland Security (DHS) in 2003. A separate division called United States Computer Readiness Response Team (US-CERT) was created within DHS with sole responsibility of securing the federal government network from any eventual attack (US-CERT, 2011).

To achieve this objective, DHS was tasked to develop emergency plans that would be used to warn and direct the network users in an event of a threat. The work of US-CERT is limited to government network users only since it had been realised that these users were not covered by already existing structures within the private sector that prevent cyber-attacks. The job of US-CERT is to provide current information about security risks and exploits through the government alert system, and then ensure that solutions are available to address the issues (Ferwerd, Choucri & Madnick, 2010).

Within the private sector, it has been identified that 97% of severe cybercrime incidents go unreported in order to avoid negative publicity to businesses. Therefore most businesses care more about protecting their reputation; hence this results in under-reporting (BERR, 2008). This trend has also been reported to be similar in the USA (Campbell et al., 2003; Richardson, 2007).

Walls (2007) further notes that organisations do not see the need to report cybercrime incidents to the police because they lack the necessary expertise to handle information security issues. This results in very few cases being taken to the police (nearly 7%), while most victims end up seeking help from professional security experts (39%) as reported in the UK (Fafinski et al., 2010).

The problem of under-reporting has also been noticed among individuals. This was revealed in a survey in UK in which it emerged that for Internet security breaches at household level, only 13% ever reported the incidents; 27% indicated they would report to their Internet Service Providers (ISP) and not to the police. This trend was found to be similar even for virus infection incidents from a British study conducted in 2004. In the case of individuals, under-reporting for cybercrime has also been attributed to fear of embarrassment and victimisation especially where there are monitory loss involved (Wilson et al., 2006).

Wall (2007) advices that in order for cybercrime reports to have an impact they should be aggregated to avoid being treated as isolated cases; this would allow the police and other agencies to form links between the incidents and identify any underlying trends. Aggregation of reported cybercrime incidents can also be used to reveal severe impacts of some attacks such as denial of service (DoS) attacks which cannot be picked from isolated reports. Therefore, this makes it easier and cheaper to respond to these incidents than attending to them in isolation (Fafinski et al., 2010).

Some of the cybercrime reports are produced by private companies who happen to be involved in the information security industry; hence they have vested interest on the impact of their reports. Therefore their findings should be interpreted with care since they might be tempted to exaggerate the state of cybercrime in the quest to promote their products or services (Wall, 2007).

2.3.1 Cybercrime Statistics

This section will provide statistics of cybercrime that have been reported by different organisations, mostly for the developed countries. These statistics are meant to give indication of the extent that this crime is affecting the information society.

Table 1 shows the rate at which criminals are sending targeted email attacks to organisations in specific sectors or industry. This report was adopted from Symantec's Internet Security Report. The government or public sector was reported as the highest targeted sector at 25%, followed by manufacturing at 15% and finance at 14% (Symantec Corporation, 2012).

Sector	Rate of Targeted Email Attacks
Retail	3%
Education	3%
Marketing and Media	3%
Non-Profit	4%
Transport and Utilities	6%
Chemical Pharmaceutical	6%
IT Services	6%
Finance	14%
Manufacturing	15%
Government and Public Sector	25%

Table 1: Top 10 Targeted Email Attacks by Sector for 2011 (Symantec Corporation, 2012)

On the other hand, Table 2 below shows the rate of data breach experienced by organisations in specific sectors or industry. In this category the health care sector received the highest rate of breach with 43%, followed by government or public sector at 14%, education at 13% and finance at 8% (Symantec Corporation, 2012).

Sector	Rate of Data Breach
IT Services	3%
Insurance	3%
Hospitality	3%
Retail	4%

Computer Software	5%
Arts and Media	5%
Financial	8%
Education	13%
Government and Public Sector	14%
Health Care	43%

Table 2: Top 10 Data Breaches by Sector for 2011 (Symantec Corporation, 2012)

Another issue that has been reported to be of much concern to most network administrator is the amount of bandwidth that is consumed by email servers to download spam emails that are flooding user's email accounts. The amount of spam emails was reported to have dropped in 2011 compared to what has experienced in 2010. Figure 1 below shows that in 2011 spam accounted for an average 68% of all emails that were received by organisations around the world (Symantec Corporation, 2012).

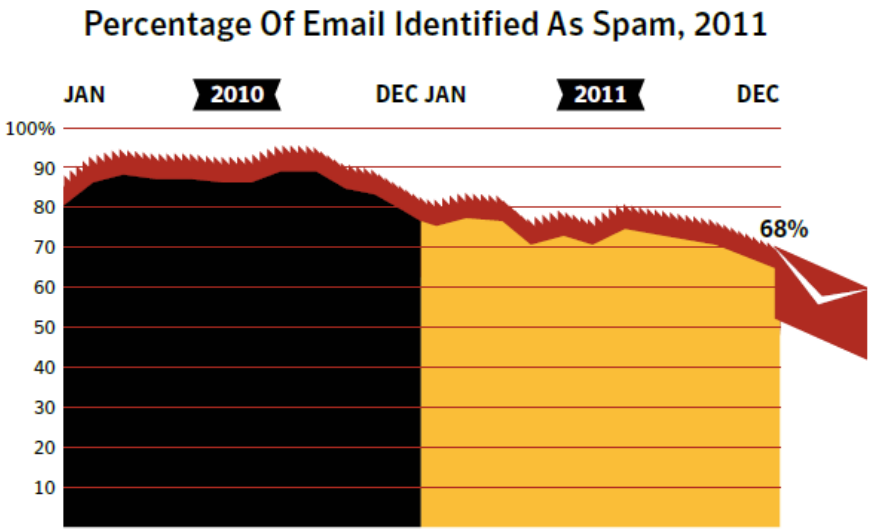

Figure 1: Rate of Spam Email for 2011 (Symantec Corporation, 2012)

Table 3 shows the types of cybercrime attacks that organisations in the USA have been experiencing from the years 2007 to 2010 as reported by the Computer Security Institute (CSI) Survey report for Computer Crime and Security report of 2011. This report indicates that most attacks have been reported to be dropping in percentage each consecutive year except for malware infection, bots and phishing attacks. This was due to the fact that CSI's

respondents are mostly companies that actively employ security tools to protect their network (Computer Security Institute, 2011).

Type of Attack	2007	2008	2009	2010
Malware infection	52%	50%	64%	67%
Bots / Zombies within organisation	21%	20%	23%	29%
Fraudulently represented as sender of phishing message	26%	31%	34%	39%
Password Sniffing	10%	9%	17%	12%
Financial Fraud	12%	12%	20%	9%
Denial of Service	25%	21%	29%	17%
Website Defacement	10%	6%	14%	7%
Exploit of social network profile	n/a	n/a	7%	5%
Internet access / email abuse by insiders	59%	44%	30%	25%
Unauthorised access by insiders	n/a	n/a	15%	13%
System breach by outsiders	n/a	n/a	14%	11%
Laptop / portable hardware theft or loss	50	42%	42%	34%
Intellectual property theft / unauthorised access	n/a	5%	8%	5%

Table 3: Experienced Attacks by Percentage (Computer Security Institute, 2011)

Tables 4 and 5 below, show the statistics that have been reported to the Japanese Police Service in 2003 regarding cybercrime since 2000 to 2002. In Table 4, the number of incidents reported to the police is presented. This shows that incidents have been increasing with each year from total complaints from 11,135 (2000) to 19,329 (2002); this reveals a significant increase in cybercrime. Table 5 also shows that the number of arrests that were made in connection to cybercrime in Japan also increased within the three years. In 2000 there were 559 arrests, which increased to 810 in 2001 and further jumped to 1039 in 2002 (Natsui, 2003).

	2002	2001	2000
Auction on the computer network	3,978	2,099	1,301
Fraud and related malicious trading	3,193	1,963	1,396
Defamation	2,566	2,267	1,884
Malicious contents	2,261	3,282	2,896
Unsolicited e-mail message	2,130	2,647	1,352
Unauthorized access, computer virus etc.	1,246	1,335	505
Others	3,955	3,684	1,801
Total	19,329	17,277	11,135

Table 4: Number of Cybercrime Complaints in Japan (Natsui, 2003)

	2002	2001	2000
Unauthorized computer access	51	35	31
Computer crimes on Penal Code	30	63	44
(Illegal electromagnetic record)	(8)	(11)	(9)
(computer interference)	(4)	(4)	(2)
(computer Fraud)	(18)	(48)	(33)
Other crimes by means of network systems	958	712	484
(prostitution of children)[9]	(268)	(117)	(8)
(child pornography)	(140)	(128)	(113)
(fraud)	(112)	(103)	(53)
(obscenities)[10]	(109)	(103)	(154)
(Intimidation)	(33)	(40)	(17)
(copyright infringement)	(31)	(28)	(29)
(defamation)	(27)	(42)	(30)
Total	1,039	810	559

Table 5: Number of Cybercrime related Arrests in Japan (Natsui, 2003)

2.4 Economic Factors of Cybercrime

Since cybercrime has been shown to be a persistent problem globally, this section will look at the economic factors that contribute to the high rise of this crime.

2.4.1 Drivers of Cybercrime

Information security concerns over the years have transformed from just hacking for 'the fun of it' by mostly teenagers to an active wealth generating underworld business; where the incentives are to make money (security-faq, 2011). Cybercrime is reported to surpass drug trafficking by the amount of money that is generated (Silicon Republic, 2009; Symantec Report, 2012). One reason why this is such a lucrative market is that perpetrators do not believe that they can easily be caught, or even convicted in case they are prosecuted. This is

because they have mastered how to conceal their digital tracks which makes it hard for enough evidence to be brought against them (Guerra, 2009).

2.4.1.1 Increase in Internet Access for Africa

The proliferation of fast Internet connections throughout most parts of the world which also connects African countries further presents an opportunity to commit cybercrime in any country (Cambini & Jiang, 2009; Grobler & van Vuuren, 2010). This situation also makes it hard for prosecution since most countries do not yet have extradition agreements for this kind of crime as shown by the failure of some cases in Botswana and other countries (Ngakaagae, 2010; Sosa, n.d).

The growth in Internet connections for Africa is shown in Figure 2 and 3 below. African countries have made significant investments since 2008 in a number of projects that were meant to increase Internet access and the bandwidth available for data communication (Cambini & Jiang, 2009; Grobler & van Vuuren, 2010). Figure 2 shows how Africa was initially expected to be connected to the international community by 2010 through undersea fibre cable like the Seacom (SEA Cable System). It is evident that this connection was limited to only a few countries. Figure 3 on the other hand shows how the outlook of undersea cables for Africa in 2011 was predicted to be; this followed the signing of a Memorandum of Understanding (MOU) in 2008 by Telcome-Orange (France) for installing a cable in the cost line of Western Africa to service over 20 countries, from Gabon to France (Cottrell & Kalim, 2009).

There has been an increase in Internet connectivity in general in Africa (Manda, 2011).
Even though the Internet brings about a lot of benefits, it also carries notable security issues, especially given that most users lack sufficient skills for cyber security and the increasing problem of cyber attacks result in heavy losses for developing countries (OECD, 2005).

Therefore, this increase in ICT and Internet connection will eventually expose government departments and corporations to increased cybercrime attacks (Arpana & Chauhan, 2012; Grobler & van Vuuren, 2010). This will further be worsened by the fact that when there is a high dependence on ICT and the Internet, it has been reported that cybercrime becomes much easier to occur since faster internet makes it easy for perpetrators to launch attacks in a short

period of time due to high speed connections (Cassim, 2009), hence there is now high interest to stop or prevent this crime (Arpana & Chauhan, 2012).

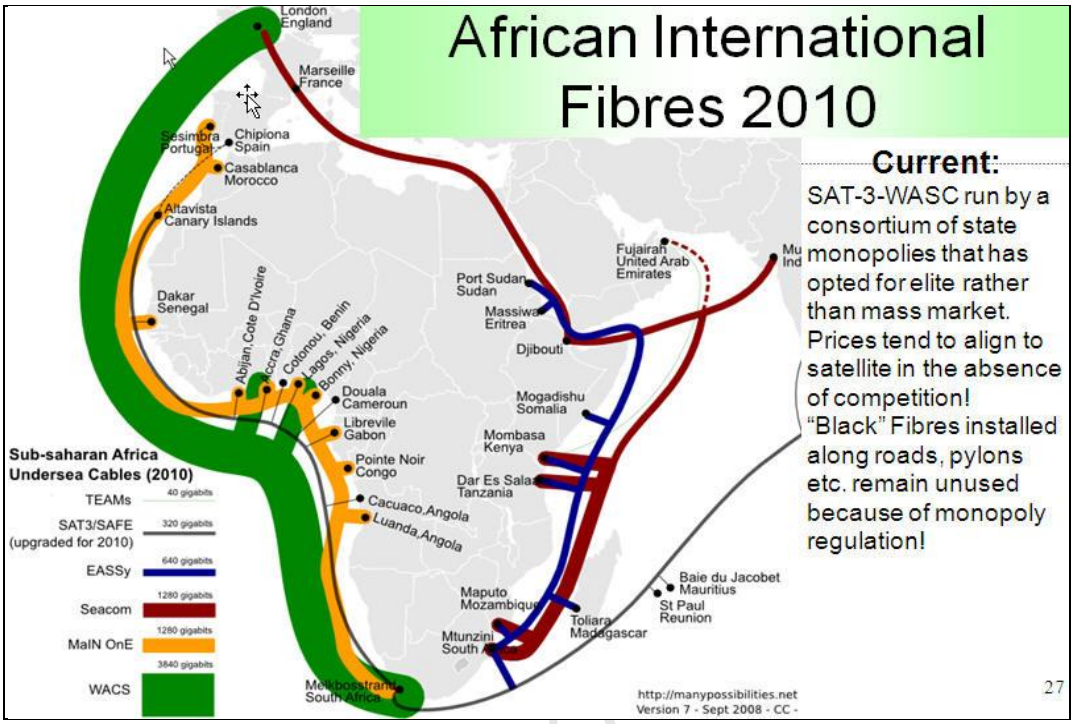

Figure 2: International Fibre Cable for Africa 2010 (Cottrell & Kalim, 2009)

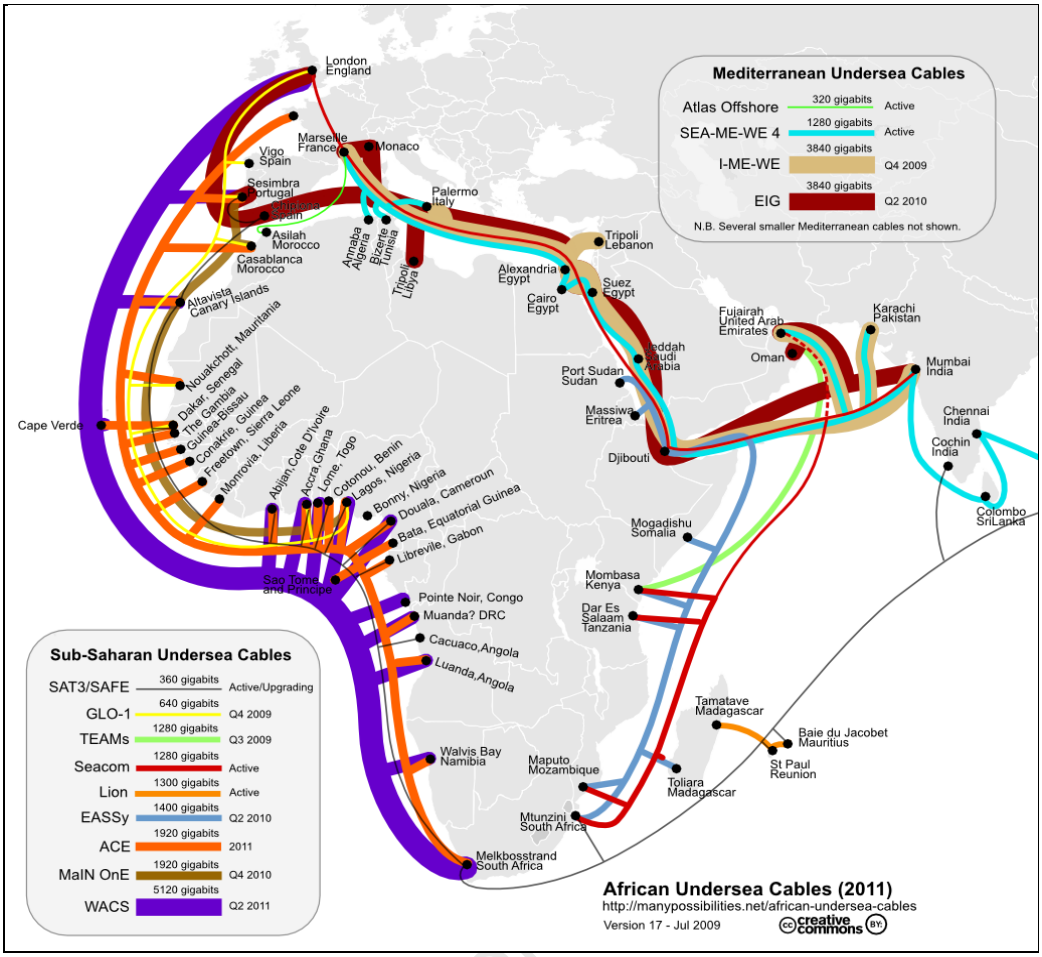

Figure 3: Resultant Undersea Cable for Africa (Cottrell & Kalim, 2009)

2.4.1.2 Technical and Intensive Skills

Cybercrime has unique factors that make it different from conventional crime. First of all, it requires technology and needs intensive skills; it is global in nature and can reach multiple targets; it is also a relatively new form of crime as compared to other crimes. These factors make cybercrime difficult and costly to manage, but on the other hand this makes it more attractive to perpetrators (Kshetri, 2006).

For someone to commit cybercrime some technical skills are required, even if the person uses readily available tools to do so; they would still need to possess more skills compared to other criminals that carry out other conventional crimes (Kshetri, 2006). Furthermore, tools needed to commit cybercrime are easily available and can be purchased at affordable prices or even downloaded for free; this makes cybercrime more attractive to commit (Hirschauer & Musshoff, 2007). This situation makes it difficult for the law enforcement to fight cybercrime since only very few of them have cyber forensics skills (Akuta et al, 2011) and new trends of cybercrime are being developed rapidly on daily bases (Symantec Corporation, 2012).

The sophistication of cybercrime makes it difficult for law enforcement to investigate, due to limitation in resources and expertise. Therefore this results in developing countries not being able to investigate all reports of cybercrime (Kshetri, 2006). For instance it was found that in Indonesia only 15% of reported cybercrime is investigated, which is further complicated by the global nature of the crime, since through ICT cybercrime is not bound to national borders; different regulations in countries also make it hard to fight this crime. A recent announcement by Interpol (International Police) that only cases of values above 6000 Euros will be investigated (Madiya, 2012) makes it difficult to fight cybercrime across countries. Countries such as China and Russia which are among key fraud generators have been reported to ignore calls to cooperate with cybercrime investigations unless if the committed crimes also impact negatively on their countries (Rosenau, 1995).

Therefore the above factors results in a few cases being investigated successfully by law enforcement, which further results in fewer cases being reported by victims since they know that there is little chances for them being successfully investigated. This then creates what Kshetri (2006) terms the vicious circle of cybercrime, which reinforces assurance to criminals that they will not be easily prosecuted which leads to poor reporting by cybercrime victims. Therefore, cybercrime becomes very attractive to perpetrators and this drives it to go on uncontrollably.

2.4.2 Cybercrime Incentives Analysis

From an organisational perspective, it is believed that cybercrime is driven by the fact that there are misaligned incentives between people who are supposed to protect the systems from breaches since they do not see any immediate need for them to do so. On the other hand due to lack of understanding of cybercrime, management might not have any incentive to allocate money that is needed to secure the system as they do not think they would be directly affected by the breach (Anderson & More, 2006). This results in management of cybercrime not receiving the deserved attention which would facilitate coming up with relevant measures and mechanisms that could best protect the information assets of organisations. Hence identifying and reporting it becomes a secondary issue and at most times is never done at all. In order to avoid such situations, certain laws and standards have been setup to guide management; corporate governance structures are one such guideline.

2.4.2.1 Corporate Governance

This sub section will look into two examples of corporate governance structures being: the King III code of South Africa and the Sarbanes-Oxley Act of the United States of America with attention to reporting guidelines that are provided to ensure that organisations adhere to set standards.

The King III code of conduct for corporate governance is a reference guide that has to be adopted mainly by all firms that are listed on the Johannesburg Stock Exchange (JSE), however the KPMG report on King III states that this code applies to all organisations regardless of whether they are in the private or public sector (KPMG, 2009). The code provides guidance to the board of directors, management, service providers and other stakeholders on recommended ways of governing the organisation; these include but not limited to board composition, setting up audit committees, risk committee for risk management, IT management and compliance. The code adopts the 'apply or explain' approach which requires organisations to implement the recommended principles and if not, give details that are in place and then explain the difference.

The Sarbanes-Oxley Act (SOX) is a United States of America (USA) regulation that was passed in 2002 by congress to address challenges that public companies were having which had resulted in low public and investor confidence. The Act brought significant changes and controls for corporate governance and financial procedures, by placing strict responsibilities for production of financial reports on board directors, managers and auditors with strict penalties for failure to comply with it (Conference of State Bank Supervisors, 2010; Soxlaw, 2006). The main reason for SOX was to bring back the confidence of investors in financial reports that were produced by firms. The Act has a number of sections and subsections but of most importance are three sections that relate with accounting. These are responsibilities of Public Companies Accounting Oversight Board (PCAOB) concerning financial reporting for firms; corporations or firms, mainly the board directors and the management; lastly the external auditors that provide services to these firms (Soxlaw, 2006).

2.4.3 Cybercrime Motivations

To have a better understanding of why individuals engage in cybercrime it would be necessary to look into what really motivates them to behave in such ways (Coates, 2002). Just like conventional crime, cyber attacks are also meant to achieve material benefits as well as

intangible ones like respect, status and supremacy (Hirshleifer, 1998). This understanding will help to explain why there is a range of cyber criminals from teenagers, intermediate hackers, to refined white-colour thieves that target large and financially strong organisations.

2.4.3.1 Intrinsic Motivations

According to intrinsic motivation theory, the driving force to do something is attributed to the enjoyment or interest that is achieved while doing it and not any external rewards (Deci & Ryan, 1985). This theory has also been used to explain why infants strive to try out new things in their environment as they discover them (Berlyne, 1965). According to Kshetri (2006) intrinsic motivation can further be grouped into two categories with some falling under enjoyment, while others fall under obligations. Under enjoyment the individual gets motivation from the fun or enjoyment that they experience while engaging in an activity. This is likened to the enjoyment that comes from playing a game that has different stages which get difficult as the player moves between the levels; hence the player will continue playing in order to advance in the game. The same satisfaction is achieved by attackers as they penetrate a system because of the challenges that they have to overcome (Kshetri, 2006).

2.4.3.2 Extrinsic Motivations

This is the opposite of intrinsic motivation, and has its roots in the economic theory which holds that human behaviour is driven by external incentives such as benefits (Frey, 1997). The anticipated benefits could either be realised immediately or at a later stage; the financial benefits that perpetrators anticipate to receive are seen to be a motivating influence for their drive to commit crime (Kshetri, 2006).

2.5 Cybercrime Awareness

This section will look at awareness of cybercrime within organisations, paying particular attention to general users to determine whether organisations put in any effort to ensure that they are made aware of information security issues. Consequences of this lack of knowledge will also be addressed. In this section the term information security awareness is used interchangeably with cybercrime awareness.

With increased change and advancement of ICT such as computer networks, cyber attacks are becoming complicated and not easy to identify (Arpana & Chauhan, 2012); this results in frequent attacks to the network due to the fact that users have little awareness of these attacks

and their impact (Veerasamy & Taute, 2009). Often emphases is normally directed towards implementing strong security tools and controls to secure the system, with less consideration for encouraging users to have a good sense of awareness towards information security matters which would prevent possible mishaps in advance (Veerasamy & Taute, 2009). Results from a recent study in India revealed the importance of instilling cybercrime awareness into users in order to prevent cybercrime. The study further reported that lack of cybercrime awareness was prevalent across all occupations and positions in organisations, and this resulted in less cybercrime reporting (Arpana & Chauhan, 2012).

Cybercrime awareness is often overlooked within the information security plans that organisations embark upon during expansion of their ICT. Most of the time they only think of training the technical professionals in charge of information security, and forget about the systems users, which leaves them as the weakest-link; hence they become the point of entry for security breaches. Lack of information security awareness combined with high speed Internet connections make organisations attractive to cyber criminals (Aloul, 2010).

According to Aloul (2010) information security incidents have increased due to the following reasons:

- A high increase in digital or electronic data due to computerisation of most services.
- An increase in the number of mobile and portable devices.
- A worldwide increase in professional cybercrime groups.
- Increase in sophisticated information security threats originating from both internal and external sources.
- The fact that it is not easy to trace most attackers.
- Lack of security awareness by computer users, especially the ones with internet access.

Aloul (2010) goes on to say that this increase in information security incidents is the driving force behind most governments' decision to introduce laws that are meant to fight cybercrime. Among the reasons why information security breaches are on the rise is that, despite the fact that organisations are adopting advanced technology to secure their networks, hackers specifically have been found to target the uninformed system users. Hence lack of

knowledge by users has been identified among the top risks for IT security (Whitman & Mattord, 2007).

Information security exploits which are carried out during an act of cybercrime occur through computer networks of organisations (Veerasamy & Taute, 2009); therefore it is important for users to understand and know the nature of these exploits in order to be aware of them.

2.6 User Training on Information Security Awareness

Aloul (2010) insists that since the hacking community is always finding new ways of stealing information from naïve users, organisations must do something to remove this weakest link in their information security plan. He suggests that users should be educated on this area and then apply this knowledge into their daily work life. Below are the points that are considered crucial for this to be effect:

- Government should come up with cybercrime laws and then ensure that they are enforced. For this to be effective there is a need for collaboration with other governments since cybercrime has no border.
- There should be Emergency Response Teams set up that would work to support and enhance awareness among organisations, and train cybercrime forensic teams which will assist in the fight of cybercrime.
- The police department should have special trained officers whose job would be digital forensic investigation.
- Organisations should provide information security training programmes for their employees and clients; this should be done on regular bases either twice a year to fight new threats that come up from time to time. This program needs management to set aside funds to support it.
- The organisation should set up a central point where all communication on information security would be directed to make it easy for user communication. This will enable the organisation to adopt a proactive approach towards information security awareness.
- General users are also encouraged to develop a spirit of continuously reading materials that address IT security matters so that they know how to protect themselves from new threats.

Therefore, in order to realise returns from investments on ICT by African countries, further investment should be done on developing the user capacity to enable economic growth (Holmner, Britz & Ponelis, 2010). One way to do this is through user training on information security measures. Limitation on education prevent users from knowing what to do when faced with cybercrime incidents, hence they have to be made aware of cybercrime trends and their effects (Grobler & van Vuuren, 2010). Furthermore, training users on information security is regarded as crucial in order for them to protect their information.

In order to create more awareness for cybercrime that will help organisations to be ready to address the problem of cybercrime reporting, the following four sections (2.7, 2.8, 2.9, and 2.10) will address concepts and theories that are a closely linked to the area of information security. Knowledge of these concepts will be helpful to organisations and if implemented it shall also enable them to easily report and investigate most cybercrime incidents that they experience.

2.7 Digital Forensic Readiness

This section will address the issue of digital forensic readiness as a need for organisations and businesses that have embraced the digital age.

Most organisations both private and public have implemented ICTs in their operations to harness the efficiency and productivity that has been commonly attributed to it (Longe et al., 2009). Unfortunately ICT also gives rise to opportunities for unforeseen information security events some of which are deliberately intended to cause harm and some are just of an unfortunate nature; nevertheless these events result in loss in one way or another, hence organisations need to prepare for them in order to have digital evidence of such events (Barske, Stander & Jordaan, 2010). In some instances once an incidence has occurred it is very difficult to locate and preserve evidence when it was of a criminal nature because intruders conceal or destroy any evidence that could easily reveal their tracks (Casey, 2006).

The situation presented by lack of readiness by organisations to collect the needed evidence to point out to what really happened to a computer system in order to seek redress from it or even investigate it, shows organisations are not digitally ready for forensics (Casey, 2006). On the other hand, organisations have started to treat security breaches more serious due to the escalation in computer systems compromise experienced. This might also have to do with

the realisation by Casey (2006: 49) that "network intrusions are among the most challenging kind of computer crimes to investigate, especially when dealing with sophisticated, highly motivated intruders... investigators must act quickly to locate and preserve potential evidence before it is lost or altered."

2.7.1 Digital Evidence

The collection and preservation of digital evidence is central for an organisation to achieve digital forensic readiness, hence it is important to understand what really constitutes digital evidence. Casey (2004) defines it as any kind of data that can be stored processed or transmitted by a computer system or any device with computing or storage capability. This data is represented by strings of bits which can be easily manipulated, therefore digital evidence needs to be collected and preserved in a specific way acceptable by law (Danielsson & Tjostheim, 2004).

In computer networked environments there are opportunities to actively gather information that could serve as evidence when the need arise. These include network log files, email communications, internet & network traffic logs, disk back-ups, transaction records, computers and laptops, server log files, anti-virus software log files, security system log files, other portable computers systems and cell phones, just to name a few. The evidence could be collected as normal routine to monitor the system and then used later after a crime has occurred (Rowlingson, 2004).

It is important to understand the sources and types of potential digital evidence of an organisation in order to collect it properly (Casey, 2006). The sources may be broadly classified in four groups namely those created by users, protected by users, created by the computer system, and other data. Files that are created by users are those data files that the user creates and saves on the computer when operating programmes on the computer. Then there are those files that the user chooses to protect either with encryptions or password to make them private and limit access to them. The third type includes data files that are generated by the computer's operating system and other programmes that are installed. The last type of other data includes any other data that enters the system or comes from outside the computer.

2.7.2 Digital Forensics

Digital forensics is defined by Zatyko (2007) as making use of computer science and investigation methods to fulfil a legal order which requires that digital evidence should be analysed according to mathematical tools and procedures then presented to court by experts in the field. This is preceded by a proper search warrant and also with safe keeping in custody for preservation. Digital forensics is delicate in nature and requires careful treatment for the evidence produced to be acceptable. First of all it has been shown from the definition that there should be legal authority for it to happen; it also requires the organisation involved in it to be prepared in order to minimize cost (Barske et al, 2010).

Vacca (2005) says the main concern of digital forensics is ensuring that accepted rules, procedures and legal requirements are followed while collecting evidence from computer systems. Therefore, this ensures that the following things can be carried out:

- Legal authority has been sought out before conducting any search.
- Keeping the evidence according to correct custody processes.
- Using valid tools to conduct the analysis of evidence.
- Conducting the analysis in a quality manner to ensure that similar results could be obtained by another expert.
- Making a proper record of the findings.
- Having an expert ready to testify on the finding in a court of law.

Digital forensic focuses on maintaining integrity towards the evidence collected, which is why the process needs to be done in the proper way that follows all set out guidelines.

2.7.3 Towards Digital Forensics Readiness

The requirements of digital forensics call for organisations to be forensic ready; this is defined by Rowlingson (2004:1) as "the ability of an organisation to maximise its potential to use digital evidence whilst minimising the cost of an investigation." When an organisation is forensic ready, this benefits it in the sense that its computer system environment has the ability to provide reliable digital evidence which also lowers costs associated with gathering evidence needed to address a given incident.

Digital forensic readiness aims to enable an organisation to be in a position to deal with any situation that can be resolved by providing digital evidence either to settle a dispute or prove otherwise in a legal proceeding or dispute (Rowlingson, 2004). The aim therefore is for organisations to set up an environment that is conducive for the collection and preservation of digital evidence (Danielsson & Tjostheim, 2004).

Rowlingson (2004) gives the following goals of digital forensic readiness:

- Collecting of digital evidence in a legally acceptable manner without disturbing the normal running of an organisation.
- Collecting evidence on activities that are prune to crime and disputes that may affect the reputation of an organisation.
- To minimise costs associated to digital investigation.
- To increase success of legal proceedings that depends on digital evidence.

2.7.4 Benefits of Digital Forensics Readiness

It has already been shown that government through the adoption of e-government has embraced the use of ICT and thus is now connected to other information users and the rest of the world through the Internet (Moloi & Mutula, 2007); hence a lot of information is now available in digital format. Therefore, this presents a more need for government and the private sector to ensure that they are digital forensic ready so that they can be able to minimise costs associated with retrieving digital evidence whenever they need it (Sommer, 2009). This also means that organisations can enjoy the ability to collect any required digital evidence without any pressure on their part since they will be assured it already exists. The gathered evidence can be used to settle issues of labour disputes and discipline for employees who have contravened any regulations (Imtiaz, 2006).

Rowlingson(2004) notes that when an organisation has set up forensic readiness program and is also active in its implementation, this can also act as a deterrence to even internal threats by employees since they would know that there is evidence collected on their activities.

Another benefit of digital forensic readiness is that the International Standard for Information Security ISO 17799 also requires that any digital evidence collected must be done according

to forensic guidelines for it to be used in any legal proceedings. The evidence collected may be for the following purposes:

- To settle internal problems within the organisation.
- To serve as digital evidence for court proceedings, breach of contract or requirements.
- Seeking redress from service providers.

(Saint-Germain, 2005).

2.8 Cybercrime Incident Management

This section is about cybercrime incidents and how they should be managed in order to address them once an organisation's information system has been attacked. It also outlines responsibilities of different people in the organisation in regard to this activity.

In order to properly address information security breaches experienced even by the public sector the breaches need to be well identified and recorded; but within the Botswana public sector this is currently a serious challenge and little has been done so far to identify them due to limited knowledge (Ngakaagae, 2010). This challenge seems to be experienced by many governments in Africa and other parts of the world; partly this is due to the fact that there is no appropriate government agency which has been tasked to deal with them and also that there exists no guideline structures to help with such a process (el Kettani & Debbagh, 2008; Ochieng, 2011).

West-Brown et al. (2003) warn that there is normally a confusion that exists between digital forensic readiness and incident management. They clarify the confusion by defining that the latter is any negative event which can breach the security of a computer system. This can be a virus infection, unlawful access to an organisation computer resource, theft of digital documents, and other similar events. Therefore, incident management deals with responding and resolving computer security incidents.

To emphasise how different digital forensic readiness is from incidence management, Mandia and Prosise (2001) outline the aims of incident management as follows:

- To find out if a security incident has occurred within a computer system.
- To support collection of information regarding the incident at hand.
- To formulate procedures to properly collect evidence related to an incident.

- To contain the interruption to the computer network and business services.
- To enable the organisation to take legal action.
- To give a proper report regarding the incident and guide for necessary recommendations.

The Department of Energy (2009) in the US government has developed a comprehensive manual that guides the entire department on cyber incidents; it can be used as a benchmark by countries which do not yet have any procedure or framework that addresses cyber incidents. The manual outlines different processes on how to identify, categorise, contain, report and mitigate incidents, and goes on to even assign responsibilities that different categories of staff members need to do. Allocation of responsibilities in this way brings a solution to the problem that is identified in the section of Economic factors of cybercrime, where top management and the IT personnel do not have incentives to adhere to security procedures. The manual outlines that management should ensure that the procedures are implemented by the units in the department, and then the IT personnel should ensure proper execution of all steps that need to be followed when an incident occurs.

When incidents are not managed properly, this results in challenges with the existing reporting methods relating to cybercrime (Smith, 2004). Therefore cybercrime reports that are made would not give a true reflection of what is really experienced (Richardson, 2007). Canhoto (2010) argues that identifying and reporting losses from cybercrime is a process that depends on a number of aspects that include having a sound knowledge of cybercrime, and also how to identify and analyse attacks.

2.9 Privacy Theory

This section looks at the privacy theory in relation to cybercrime, especially in the context of the public sector and its handling of citizen's information. It also examines how this has been affected by ICT.

Privacy is not well understood in relation to where it starts and stops, and this has now been made harder by the adoption of ICT for storage and processing of information. Moor (1997) describes information that has been digitised as "greased" information and says it slides easily to any place where it is directed to go to and once in this state the original owners of

such information have no control at all to what happens to it. The issue of privacy arises when improper exposure and utilisation of information occurs without even the knowledge of its owners or custodians. Altman (1975, 67) defines privacy as a regulated process of "selective control of access to the self" by imposing boundaries which affect how much information about a person is accessible per given time.

Palen and Dourish (2003) bring up the issue of privacy management and argue that it is not necessarily about making rules about one's privacy but more of managing the boundaries (rules or limits) at different times, places and situations of how much information is disclosed; boundaries reflect differences in conflicting goals between different actor and stakeholders such as the public and government in relation to information held about citizens.

Privacy concerns have been complicated by the introduction of ICT in most government operations to enhance service delivery, such as the e-government initiative that Botswana government has embarked on where a lot of information is now computerised and can move through the system very easily. Palen and Dourish (2003) argue that this results in a disturbance in the control of boundaries of privacy in several ways: it can enhance the process of boundary controls; it can change the boundaries; it can serve as a means to manage the boundaries and also help to make it easy for participation across the boundaries. The main concern is due to the fact that some of the information that is captured by government is highly sensitive and private therefore would require to be protected against unauthorised access which would be a difficult challenge with the current situation of high corruption, poor controls and less experience in incident management (Ngakaage, 2010).

2.10 Risk Management

This section addresses the risk aspect of digital information, and also how risks should be managed in the public sector.

When information is digitised and availed through ICT, an element of risk is created in the sense that its confidentiality, integrity and availability might be compromised; such a compromise of valuable information results in a loss by the owner. This loss could be direct (devaluation in information value) or indirect (legal action, loss of reputation or service disruption) to the organisation (Blakley et al (2001). A risk is defined as a possibility of an

event that would result in a business losing its value if it occurred; hence a risk has a cost associated to it which can be quantified (Harrington, 1999; Department of Treasury and Finance, 2007). Management of risks in business is done on a daily bases using either of the following: liability transfer, indemnification, mitigation and retention (Blakley et al, 2001). Volk (2010) advises that the best risk management method to use is the threat based approach which he contends, easily quantifies threats and produces a Return of Security Investment (ROSI) which makes it easy to use the best controls to reduce risks.

Risk management seems to be working fairly well for the private sector from which governments can learn a lot and apply different techniques to manage their risks in order to achieve their goals (Volk, 2010). The objective of government is not to make profit, but rather to provide services to the public. There are a various departments and stakeholders that are involved in providing such services, who have different interests; hence this situation results in challenges with conventional risk management principles (Cameron & Stone, 1995).

With the utilisation of ICT in service delivery to the public, risks that were once treated separately are now related as different processes are linked together in the provision of services; these risks cannot be treated separately. Therefore the public sector needs to adopt sophisticated systematic risk management approaches that can enable it to achieve its organisational goals by assigning duties and responsibilities in the risk management process, where risks will be identified, classified, evaluated, treated, monitored and communicated to the entire organisation (Department of Treasury and Finance, 2007). Figure 1 below is a diagram that depicts the risk management process which the public sector can adopt for this function in order to make it easy to record and properly report on cybercrime. This process details all the steps that should be followed when conducting risk management.

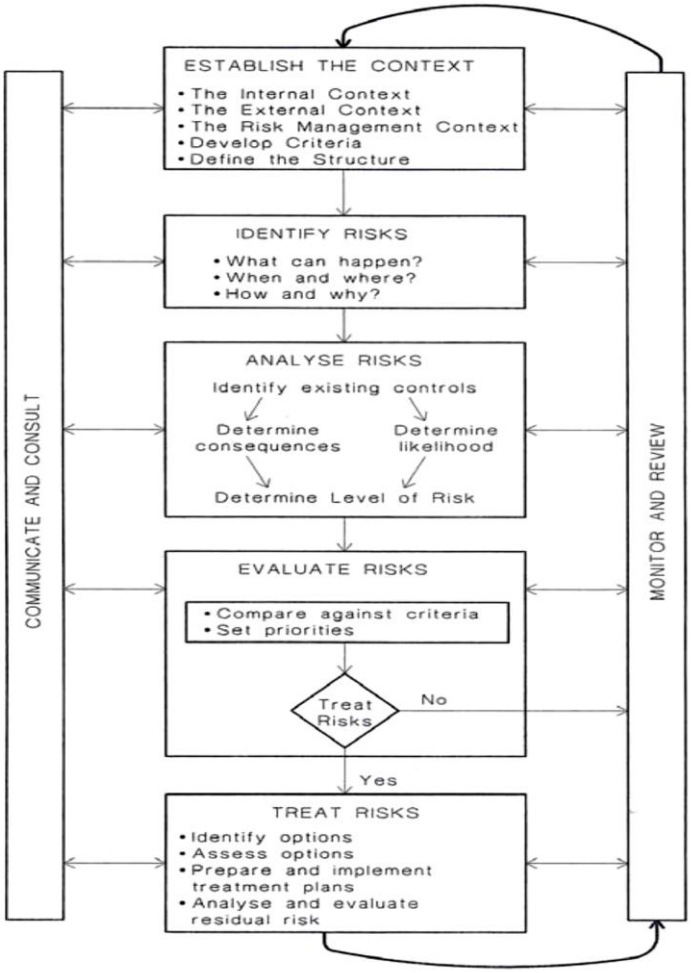

Figure 4: Risk Management Process (Department of Treasury and Finance, 2007).

2.11 Organisational Culture and Information Security Culture

This section looks at organisational culture in general and also how it impacts on organisational performance, as discussed by different authors; a link between organisational culture and security culture is also established to see how the former impacts the latter.

2.11.1 Definition of Culture

Culture like cybercrime is defined in different ways. Generally it is perceived as the collection of common traits that have an influence on a group of human beings and how they respond to their environment; it also brings about social norms and values which affect people's behaviour and beliefs (Hofstede & Hofstede, 2004). Other authors have also defined culture; Becker and Geer (1970) say it is those familiar understandings that are articulated in language; while Martin and Siehi (1983) say it is the collective pattern that are found within meanings.

Culture is believed to have the power to shape the behaviour of a group of people (Hofstede & Hofstede, 2004) in the sense that from their culture people can turn out to behave in a certain way in a given situation. Parson (1999) says that cultural values keep changing with time to incorporate new meanings or to reshape the accepted values. Therefore, the introduction of ICT in the work place can be a factor that brings in change to the culture of users which can result in the users incorporating it into aspects of their norms and values. Culture has three levels: individual, organisational and national which are different from each other (Parson, 1999). This study will focus on organisational culture to determine its impact on employees' awareness and reporting of cybercrime.

2.11.2 Organisational Culture

Organisational culture is defined in a number of ways by different authors: Martin and Siehi (1983) say it is a thread that keeps an organisation together based on the shared patterns of meaning, while Uttal (1983) sees it as those common values and beliefs that move within an organisation's policies or guidelines and result in behavioural patterns. Pettigrew (1979) saw organisational culture to be made up of cognitive systems that define the thinking, reasoning and decision making process of people in an organisation which in turn affects how they conduct their business.

Organisational culture was given much attention in the last two decades because of the effects and potential impact to bring success to organisations (Rashid, Sambasivan & Johari, 2003). Organisational culture became of interest to organisational studies around 1970 – 1980, and was thought that it could give an understanding to how some organisations performed poor than others even though they operated under similar conditions. Much research interest has since been generated to determine how norms and values guide employees' behaviour for organisations to achieve their goals (Deal & Kennedy, 1982). Furthermore, other researchers of organisational culture found out that culture was responsible for guiding and shaping the attitude, behaviour and actions of employees (Schein, 1985; O'Reilly and Chatman, 1996; Burnes, Cooper & West, 2003)

2.11.3 Impact of Organisational culture on Information Security Culture

There has been growing interest on the impact of organisational culture on information security culture; hence government departments and organisations in charge of regulations have started to show concern in understanding how organisational culture can enhance information security culture. This interest was motivated by the realisation that no matter how comprehensive the security policies are, they are influenced by attitudes and behaviour of employees in an organisation (Malcolmson, 2009). Van Niekerk and Von Solms (2009) also note that systems that are required to enforce security policies mostly depend on human attitudes and behaviour; hence humans pose the greatest threat.

The following working definition is presented for security culture:

> "… the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact" (Malcolmson, 2009: 361).

However Malcolmson (2009) also points out that there is not yet an accepted definition of security culture; hence it is still difficult to measure security culture because currently it is focused on specific characteristics of culture. Nevertheless, it is believed that if information security is considered to be a critical success factor for an organisation then paying particular attention to it is likely to lead to better performance.

In most cases, the security culture in a given organisation is a result of informally learnt practices that are passed from one employee to another during the natural process of socialisation which is usually uncontrolled. This often leads to security behaviours, attitudes and actions that have not been approved by management of the organisation. Hence if there is no shared culture towards information security matters among employees then the security system would be rendered as insufficient (IAEA, 2008). Therefore, it should not be simply assumed that employees possess enough knowledge needed to enable them to perform their duties in a manner that is secure. Instead organisations should treat security culture as a component of the existing general organisational culture (Van Niekerk & Von Solms, 2009).

Employees play a critical role for the success of any organisation, however if they are ignorant regarding information security issues they become the weakest link in the system.

This has been noted from the number of security breaches that involved insiders as compared to outsiders of the system; most of these incidents were found to be accidental and not malicious due to ignorance regarding security guidelines (Vroom & Von Solms, 2004). Therefore, to achieve a smooth assimilation of information security into the organisational culture, securing information should be integrated into the daily activities and behaviour of employees (Thomson, Von Solms, & Louw, 2006).

Malcolmson (2009) concludes that management in organisations should adopt a culture that is meaningful to their environment in order to respond to security threats, and they should formulate policies and practices which all employees will be aware of and adhere to; the culture should not be a result of informal learning between the employees since this will not be shared by everyone.

2.12 Cybercrime Legislation and Regulatory Framework

In this section the regulatory framework and laws that are needed to address cybercrime are considered.

There is a need to have the right laws which specify what actions are prohibited and amount to crime hence punishable by law (Manda, 2011). Research has however shown that introducing cybercrime laws cannot guarantee the elimination of cybercrime incidents; despite the availability of such legislation, cybercrime is still on the rise due to limitations by these legislations (Grobler & van Vuuren, 2010). Due to the technological nature of cybercrime, it is not easy to use conventional law enforcement techniques to deal with it; therefore, new tools and up to date legislation need to be developed to address the situation (Brenner, 2004; Cassim, 2009).

One of the challenges found with African countries regarding cybercrime relates to failure to develop timely legislations and regulatory framework that encourage secure use of ICT. Since cybercrime has no national boundary, its fight has since been escalated to even fall under global organisations in order to give it more weight. However, this has not yet resulted in stronger cybercrime laws that can be used to tackle the problem on a global scale (Shackelford, 2009). Nevertheless, organisations like the UN and Council of Europe have developed notable initiatives to contribute towards this fight.

2.12.1 United Nations

The UN through its resolutions made a number of recommendations to fight the misuse of ICTs by criminals. This was first done in the 1990s by UN resolution 45/121 which encouraged member states to increase the efforts to fight computer crimes. Another UN Resolutions, 55/63 and 56/121 were passed in 2001 to address the criminal misuse of ICTs; these called for development of a framework to fight cybercrime on a global scale. Two more resolutions were passed in 2002 (57/239) and 2004 (58/199) which both sought member states to enable a global culture that keep the cyberspace secure and also protect their critical infrastructure. To coordinate these resolutions easily the International Telecommunications Union (ITU) further developed a toolkit (Toolkit for Cybercrime Legislation) that can be used by all member states to develop their own national cybercrime legislation that are globally focused to operate with other existing laws (ITU, 2009).

2.12.2 The Council of Europe (CoE)

The Council of Europe started with only 10 European member countries in 1949, but now has 47 in total including non-European countries (United States, Japan, Canada and South Africa). Its goal is to develop common democratic principles for use throughout its member countries. One of its objectives includes aligning cybercrime laws and making sure that law enforcement agents and investigators follow the right procedures and techniques to solve cybercrime (Council of Europe, 2012). To fulfil its objectives, it initiated to develop cooperation efforts towards international cybercrime management on the already existing Cybercrime International Treaty in 1997. This resulted in the release of the 22nd draft (treaty) in 2000, which was followed by voluntary guidelines meant to support the collaboration work between law enforcement agents (police) and Internet Service Providers (Marion, 2010).

The intention of the CoE is to assist its member states and other non-member countries to use its convention in the fight for cybercrime. To achieve this, the organisation even goes an extra mile of translating the convention into local languages for countries that need to develop their own cybercrime laws; examples include Lao and Cambodia (Kirk, 2009). This has resulted in a lot of countries worldwide using the convention as a standard to come up with their respective computer crime legislations (COE, 2009).

Despite the involvement of UN and CoE in development of cybercrime laws, many developing countries still face challenges related to developing and implementing their own legislation. Similarly, cybercrime of different countries do not recognise the same acts as a crime; hence it has been found to be difficult to prosecute crimes that are conducted in foreign countries (KShitri, 2006). Therefore, this still poses serious challenges for addressing cybercrime.

2.13 ICT Adoption in Government

2.13.1 Government vs. Governance

This section will look at government and governance to give an understanding of how they relate to one another which hopefully will make it easier to deal with ICT governance within the public sector.

The terms government and governance have the same origin but mean different things (Kyobe, 2010; United Nations, 2007; Deloitte, 2011). Government refers to the institution or organisation that has been given the mandate to have authority to direct a country or organisation (Kyobe, 2010). The government's primary goal is to serve the needs of its citizens, thereby insuring governance (Deloitte, 2011). Therefore, governance refers to the processes, guidelines and structures that provide directions to the executive management on how to better serve citizen needs efficiently, effectively and equitably. In this regard governance provides control and accountability to the ones that are in government (Deloitte, 2011; OECD, 2005).

In order to avoid corruption and abuse of power by government, citizens and different stakeholders have begun to demand for more transparency and accountability in all processes and activities (Deloitte, 2011; Kyobe, 2010). This demand has been legitimised by results showing that good government performance is strongly related to good governance from a study conducted by the World Bank (Deloitte, 2011). This showed that organisations with good governance procedures can be expected to manage even their computer systems properly which would benefit them by having efficient controls to deal with information security management.

2.13.2 E-Government and Governance

This section looks at e-government (Electronic Government) and its impact on governance; it will define the term e-government and then briefly outline how it started within government and also how it altered the provision of services to citizens.

E-government is defined as the utilisation of ICT by government to deliver services and also enhance citizen participation in a more efficient and effective way (Lipchak & McDonald, 2003; Moloi & Mutula, 2007). In simple terms, e-government is seen as providing government services online. This seamless delivery method of services to citizens has been found as a better ways to reach many people including those in remote areas; hence governments have found it to be favourable since it makes governance much easier (Moloi & Mutula, 2007).

E-government initially appeared in the form of static information that did not require any processing of information before being delivered to citizens. This normally involved one-way communicative information from service providers pertaining to different services that they offered to people which was published in government websites. Later on government began to use ICT to carry out certain transactions with businesses that provided services to it; this ushered in the real use of on-line transactions within government, mainly for purposes of purchasing goods from suppliers within controlled data networks created only for this purpose (Moloi & Mutula, 2007).

The introduction of the Internet and the World Wide Web later provided another opportunity for wide variety of services and interaction to occur between government and both citizens and the wider business community in a more open and efficient way. This new method of service provision seemed to help make governance much better for citizens since it minimised the need for frequent visits to government offices for services that could now be reached online; such as applying for different permits, completing tax returns, applying for passports and other national registration services. This increased transparency, eliminated opportunities for bribes and also reduced the amount of time taken to provide services (Kyobe, 2010).

The above mentioned benefits that have been provided by e-government however are threatened by poor security measures that exist within the public sector (Kyobe, 2010;

Ngakaagae, 2010); hence information security on the government network will have to be enhanced in order to encourage citizens to feel comfortable while utilising services that are offered to them.

2.13.3 Corporate Governance

In order to address the issue of information security for e-Government the following section will look into corporate governance structures, notably the King III code of South Africa, to have an insight at how this might help in addressing ICT governance to minimise risks that might arise from using ICT to deliver services.

2.13.3.1 King III

The King III code of conduct for corporate governance is a reference guide that has to be adopted mainly by all firms that are listed on the Johannesburg Stock Exchange (JSE), however the KPMG report on King III states that this code applies to all organisations regardless of whether they are in the private or public sector (KPMG, 2009). The code provides guidance to the board of directors, management, service providers and other stakeholders on recommended ways of governing the organisation; these include but not limited to board composition, setting up audit committees, risk committee for risk management, IT management and compliance. The code adopts the 'apply or explain' approach which requires organisations to implement the recommended principles and if not, give details of theirs and then explain the difference.

2.13.3.1.1 Internal Audit

Under this section the organisation is required to have an internal audit unit whose duty is to ensure that the organisation is governed well, risks are managed and also having internal controls. A written report of assessment of the organisation has to be given to the board and the audit committee (KPMG, 2009; Price Water House Coopers, 2009).

2.13.3.1.2 Risk Management

Risk management is treated very serious in King III to the extent that this responsibility is given to the board to govern all risks processes by designing and implementing a risk management and monitoring plan. This enables the board to have enough time to familiarise

itself with all risk scenarios that the organisation may encounter before handing the plan to management to execute it (KPMG, 2009; Price Water House Coopers, 2009).

2.13.3.1.3 IT Governance

IT governance in King III is also made to be the responsibility of the board, where the board needs to ensure that there is a well-defined IT charter, policies and internal control framework that direct the usage of IT in general. This is meant to ensure that IT is aligned and thereby sustains the performance objectives of the organisation; the board is then required to delegate the implementation of the IT framework to management directly and may also hire a suitable IT manager with an option of having an IT steering committee to oversee the overall IT framework (Price Water House Coopers, 2009).

King III also put responsibility of ensuring that the organisation's information assets are managed in a way that provides security to the whole IT system in accordance with IT regulations and standards. Furthermore, management is tasked with ensuring that the organisation has an IT disaster recovery plan which can be used to return normal business operation in case of any disruption. Therefore, the risk committee has to be certain that IT risks are sufficiently covered in their assessment; the audit committee should also have IT issues reflected in the financial reports (KPMG, 2009; Price Water House Coopers, 2009).

2.14 State of ICT in Botswana Government

The following section will look at the state of ICT in Botswana with an aim to bring an understanding of how it has been setup and also how this has affected the e-government initiative and information security.

2.14.1 Overview of Botswana

Botswana is a landlocked country in Southern Africa; sharing borders with four countries: Namibia, Zambia, Zimbabwe and South Africa. Its surface area is around 581, 730 km^2; roughly the same size as France or the state of Texas in USA. Most parts of Botswana are a desert with less people while more people live in towns and big villages; the population is about 2 million people. The capital city is called Gaborone, and English is the official language (Republic of Botswana, 2010; IST-Africa, 2012).

Botswana gained independence in 1966, and was rated as one of the poorest nations in the world. With the discovery of diamonds, this boosted the economy to grow very much and has since made the country to maintain one of the highest economic growth rate in the world (Mutula, 2002; OECD, 2008). Following the global recession of 2008 and other political changes that affected diamond sales globally, Botswana decided to diversify its economy away from mining and towards other sustainable sectors (IST-Africa, 2012).

2.14.2 National ICT Policy

The diversification resulted in Botswana focusing into the area of Science and Technology to enable it to have an economy that is driven by innovation (Mutula, 2002). An ICT Policy called "Maitlamo" was then developed and later approved by parliament in 2007; this would be used to direct the national ICT development. The policy was also seen as a guideline that would be used to transform the country economically, socially, culturally and politically in order to achieve objectives outlined in the national vision called "Vision 2016". Maitlamo Policy was drafted in 2005 with input from various stakeholders, with an aim to provide strategic elements that will help the country to achieve its targets for national ICT development for both the government and private sector. The main key goals of the policy are: 1) To create a conducive environment for the expansion of ICT sector in Botswana; 2) to provide universal access to services and facilities of ICT in Botswana; 3) to position Botswana as a Regional hub for ICT services and enable the country to be competitive globally (Republic of Botswana, 2007).

The Maitlamo Policy has the following key projects that have been outlined and need to be achieved in order to fully realise the objectives as set out in the policy; these are further elaborated below:

- Establishing community programmes (Community Access Centres).
- Putting government services on-line (e-government).
- Establishing an online learning portal (e-education).

2.14.2.1 Community Access Centres

The goal of the program for connecting communities was to provide affordable ICT access to local people in rural and disadvantaged areas, as well as urban centres. This was meant to help people with no access to computers and internet to be able to use them. It has resulted in Community Access Centres to be established in most parts of Botswana in areas like public libraries, schools and other suitable places with facilities to sustain them (Republic of Botswana, 2007).

The government signed a contract with Botswana Telecommunications Corporation (BTC) of P350 million (US$50.1 million) in 2009 to expand the telecommunications infrastructure and services throughout remote areas in the Botswana to provide high speed internet connection (Bwalya, 2010). The purpose of these centres will be to provide access to a variety of services and information on-line such as government services and information on education, civil registration, agriculture, passport applications, health information and others. Furthermore, there will be local tailored information and services that serve each particular community according to the different categories and needs such as: age, business interests, social needs and others (Republic of Botswana, 2007).

2.14.2.2 Government Services On-line

Through the Maitlamo Policy Botswana Government sought to transform its operations to embrace the digital age by introducing a major change to the public service delivery, in order to improve the quality of services, reduce red-tape and also increase efficiency. To realise this vision, government established an e-Government initiative to be delivered through a state of the art e-Government portal for easier public access to government services. This platform will be accessed by most citizens that have internet access at their home or workplace, internet cafés as well as the Community Centres provided at most rural areas (Botswana Government, 2007).

Some of the Government services that have been put on-line include the following:

- Vehicle registration and licence applications.
- On-line payments.
- National Identity (Omang) applications.

- Passport applications.
- School registrations.
- Business application services
    - Company registration
    - Tax return
    - Credit application

(Botswana Government, 2007).

2.14.3 ICT Infrastructure Development

2.14.3.1 Fibre Optic Linkages

In order to position itself as a major player in ICT regionally and also to maximise realising benefits from ICT such as cheaper bandwidth, Botswana Government joined other countries in the region and invested substantially around US$71.6 million for the installation of fibre-optic cable to provide a link to the undersea West African Cable System (WACS) through London (shown in Figure 1). Furthermore, there was another investment into the Eastern Africa Sub-marine Cable System (EASSy) which cost around US$210 million (shown in Figure 2). This project would improve bandwidth connectivity for most countries in the region (Bwalya, 2010).

Botswana has yet other two connections that link it through fibre cables to international regions with at least 622 Mbps (STM4) via South Africa, radio link with Namibia (PDH), Zambia (622 Mbps) and also Zimbabwe (SDH). There are arrangements to further link Botswana to the private undersea cable by SEACOM in Kenya (shown in Figure 1), which has investors in South Africa, Botswana, Kenya and overseas. These investments by Botswana into such ICT infrastructure have opened more opportunities for efficient communication channels in the country (Bwalya, 2010).

2.14.3.2 Botswana Government Data Network (GDN)

Botswana Government has its own data network that connects all government departments in the whole country. The GDN is run and maintained by the Department of Information Technology (DIT). Through the GDN the government provides its own internet access

through high-speed satellite linkages to provide connection for different departments across the country to applications that are hosted centrally. The GDN depends on a primary backbone of 34Mbps, ATM links and leased lines of E1 to provide the high speed data links. Several applications that are hosted by GDN include the following:

- National Identity registration (Omang).
- Vehicle registration and licensing.
- Accounts and revenue system.
- Personnel and Human Resources System.
- Patient Management System (National Patient Database).

(Bwalya, 2010).

Figure 5 below shows the ranking of African countries as far as e-Government is concerned. The ranking results indicate that Botswana was ranked as number 117 in 2010 compared to 118 in 2008; an improvement by one point. The e-Government index for 2010 was 0.3637 which was on the eighth position in the African continent. However, when compared to countries located in Southern Africa, Botswana came second after South Africa, as can be seen in Figure 6 below.

Country	E-Government 2010	Rank 2010	Rank 2008	Rank Change
Tunisia	0.4826	66	124	+58
Mauritius	0.4645	77	63	-14
Egypt	0.4518	86	79	-7
South Africa	0.4306	97	61	-36
Seychelles	0.4179	104	69	-35
Cape Verde	0.4054	108	104	-4
Libyan Arab Jamahiriya	0.3799	114	120	+6
Botswana	0.3637	117	118	+1
Lesotho	0.3512	121	114	-7
Gabon	0.3420	123	129	+6

Figure 5: E-Government Ranking for Africa: Source (United Nations, 2010)

Country	E-Government 2010	Rank 2010	Rank 2008	Rank Change
South Africa	0.4306	97	61	-36
Botswana	0.3637	117	118	+1
Lesotho	0.3512	121	114	-7
Namibia	0.3314	125	126	+1
Swaziland	0.2757	145	125	-20

Figure 6: E-Government Ranking for Southern Africa: Source (United Nations, 2010)

2.15 Cybercrime Reports in Botswana

This section gives an outline of cybercrime incidents that have been experienced in the Botswana public sector.

The government of Botswana has only a few reported cases of computer related crimes due to the fact that as already mentioned there is lack of experience in this section which may result in many cases not being identified at all (Ngakaagae, 2010). However, in 2008 the Botswana Government was defrauded of about P17 million as payment for three separate orders for drugs which were supposedly ordered and delivered to the government Central Medical Store (CMS) (Botswana Gazette, 2008; Mmegi, 2011).

Even though there are no documented statistics for malicious code attacks and virus infections (Ngakaagae, 2010), it is generally expected that some of the public sector users have suffered from this before. The Botswana government through the e-Government strategy began developing websites for different ministries, even though this was a good initiative most of these websites were developed without even taking clients' needs into consideration; as a result they did not conform to any unified standards (Moloi & Mutura, 2007). The simple design that was adopted for these websites also poses a serious information security risk since no web standards have been adopted; this could even result in undermining crucial web security standards and rendering the websites to be easily penetrated by perpetrators.

2.16 Botswana Cybercrime Legislation

This section talks about the cybercrime law that is available in Botswana that was adopted and passed by parliament to deal with cybercrime.

The government of Botswana through parliament enacted the Cybercrime and Computer Related Crimes Act NO.22 in 2007. This act was modelled from the Convention of European (CoE) on Cybercrime even though Botswana has not yet signed the CoE (Ngakaagae, 2010; Schwarz, 2007). The Act is comprehensive in its address of this crime and is divided into the following sections:

Part I called **preliminary** is a definition of all the terms that are used in the Act. It is interesting that this section even though it contains all terms used, it however omits defining what cybercrime itself means but only addresses the different offences that constitute cybercrime. These are as follows:

Part II covers **Offences** as identified in the Act and also the penalty for each offence. The Act is very specific in the description of the offences as they are written in plain language that can be easily understood by most literate people; this avoids any misinterpretation that could occur. Below is a list of all the offences that are covered:

- Unauthorised access to a computer or computer system.
- Unauthorised access to computer service.
- Access with intent to commit an offence.
- Unauthorised interference with data.
- Unauthorised interference with a computer or computer system.
- Unlawful interception of data.
- Unlawful possession of devices or data.
- Unauthorised disclosure of password.
- Damage to a computer or computer system.
- Protected computers.
- Cyber extortion.
- Cyber fraud.
- Electronic traffic in pornographic or obscene material.
- Unlawful disclosure by service provider.

- Attempt.
- Parties to an offence.

(Republic of Botswana, 2007)

Part III covers the **Procedural Powers** that the Act provides for the law enforcement officers which are given under the orders of the commissioner of the police to collect and/or preserve any computer system that might be involved in any computer crime as evidence to be used during a trial. Below are the different elements that are included under this section:

- Preservation order.
- Disclosure of preserved data.
- Production order.
- Access, search and seizure.
- Real time collection of traffic data.
- Deletion order.
- Acting without an order.
- Limited use of disclosed data and information.
- Non-compliance with order or notice.

(Republic of Botswana, 2007)

In order for this Act to be effective and utilised, it is important that incidents of cybercrime or computer-attacks should first be identified using methods that are acceptable so that the law enforcement officers can be able to present them as evidence in a court of law and/or government to use them to estimate losses incurred (Ngwakaagae, 2010). If that is not done the Act would not achieve its intended purpose. Another crucial aspect that needs to be carried out is employee education and awareness of this Act in order for them to be aware of what cybercrime in the context of Botswana entails so they can be able to know which activities are deemed as offences, and therefore be able to report them.

2.17 Identified Gaps

The studies that have been reviewed in the literature above have identified and agree that cybercrime is a global problem that threatens the information society. Furthermore, they have identified different factors that contribute to the wide spread of cybercrime. However, most

of the studies that were reviewed are focused mostly in the developed countries; hence there is still a need to look at the problem of cybercrime within developing countries especially Africa, since these countries are relatively new on the information society. As a result they have a different understanding of ICT, and the context under which they operate is also different.

Another limitation identified in the literature was that, even though the studies identified the factors that contribute to cybercrime; these factors have been looked at in isolation from other factors that are identified by other studies. Hence, there is still a need to build a framework that looks at these factors together in order to build a consolidated solution. Furthermore, there is currently little work that has been done to address cybercrime within public sector organisation, as most of the studies tend to focus more on private organisations.

Therefore, in Botswana where the public sector has been shown to be the main driving force for developments and economic stimulation, it is then important to address cybercrime in this sector which has adopted ICT and also the e-government initiative. From previous studies, a comprehensive solution could not be found that can help address this sector, especially in a developing African country context. Therefore, this study attempts to fill this identified gap by investigating the different factors that contribute to cybercrime; it also goes an extra mile to put them into a framework and empirically validate it so that it can still be tested in other similar environments.

Chapter 3: Research Model and Hypotheses Development

This section uses the literature review in the previous chapter to develop a research framework for cybercrime reporting. The framework was developed after considering different factors that were reported by other authors as important items that are needed to improve the ability for users to report cybercrime attacks. The components considered for this model include organisational culture, cybercrime awareness, user training on information security awareness, and understanding of cybercrime legislation which have an impact on cybercrime reporting.

The research framework will be restricted to measure the relationship between the constructs in one direction only as represented in Figure 7; hence it will seek to find significant positive relationships between these constructs. The framework is explained in the following paragraphs.

3.1 Research Model Explanation

To elaborate more on the identified components for the research framework; organisational culture was included due to the impact that authors noted such as Malcolmson (2009), who reported that no matter how comprehensive the security polices for an organisation maybe, they are influenced by the culture of employees within that organisation. Uttal (1983) described it as common values and beliefs that move within an organisation's policies or guidelines and result in behavioural patterns. It was further noted that if there is no shared organisational culture towards security matters among employees then the security measures would be rendered as insufficient (IAEA, 2008). Therefore the link between organisational culture with cybercrime awareness and reporting was considered worth exploring.

Furthermore, Malcolmson (2009) who noted that organisational culture has an impact in the successful enforcement of security on information systems in organisations; as a result management should formulate policies and practices that enable employees to be aware and adhere to information security measures.

Cybercrime awareness was included based on such authors as Arpana and Chauhan (2012) who reported that due to increased change and advancement of ICT and computer networks,

cyber attacks have become complicated and not easy to identify; hence this has resulted in frequent attacks to the network due to the fact that users have little awareness of these attacks and their impact (Veerasamy & Taute, 2009). Arpana and Chauhan (2012) presented results from a recent study in India which revealed the importance of instilling awareness into users as a way to prevent cybercrime. The study further found out that lack of cybercrime awareness was prevalent across all occupations and positions in organisations hence this contributes to less reporting. Aloul (2010) also reported that cybercrime awareness has been found to be normally overlooked within the information security plans that organisations embark upon during expansion of their ICT.

Another item included in the research framework was user training on information security awareness. In order to realise returns from investments on ICT by African countries, it was noted that further investment should be made towards training system users (Holmner, Britz & Ponelis, 2010). One way identified to achieve this was through user training on information security measures. Limitation on education has been found as preventing users from knowing what to do when faced with cybercrime incidents; hence they have to be made aware of cybercrime trends and their effects (Grobler & van Vuuren, 2010). Furthermore, training users on cyber security has been regarded as crucial in order for them to protect their information. User training on information security could help to fight cybercrime by making them more aware of these attacks or risks and also emphasizing on the recommended solutions (Manda, 2011). Cassim (2009) also noted that uninformed users make an environment that is conducive to devastating attacks on an organisation's ICT.

The final component was that of understanding cybercrime legislation. A number of authors (Cassim, 2009; Grobler & van Vuuren, 2010; Manda, 2011) have highlighted the need for comprehensive cybercrime legislation that is needed to manage and control cybercrime. Ngakaagae (2010) also noted that challenges have been identified by both the law enforcement agencies, prosecutors and the general public to understand the law related to cybercrime as one of the impediments that hinder proper handling of cybercrime incidents and cases. Nyanda (2010) also reiterated the fact that a lack of understanding of the computer crime law hindered the police and government to fully control cybercrime.

Table 5 below provides a specific explanation to the constructs contained in the framework.

Construct	Description
Organisational Culture	The shared norms, values, procedures and behaviours of employees in the organisation.
Cybercrime Awareness	The extent to which users have knowledge about cybercrime.
User Training on Information Security Awareness	The extent to which users have been given training on information security matters.
Understanding of Cybercrime Legislation	The knowledge of cybercrime legislation that users have.
Cybercrime Reporting	The ability of users to report attacks from cybercrime in the organisation.

Table 6: Research Framework with Hypotheses

The research framework is represented in Figure 7 below:

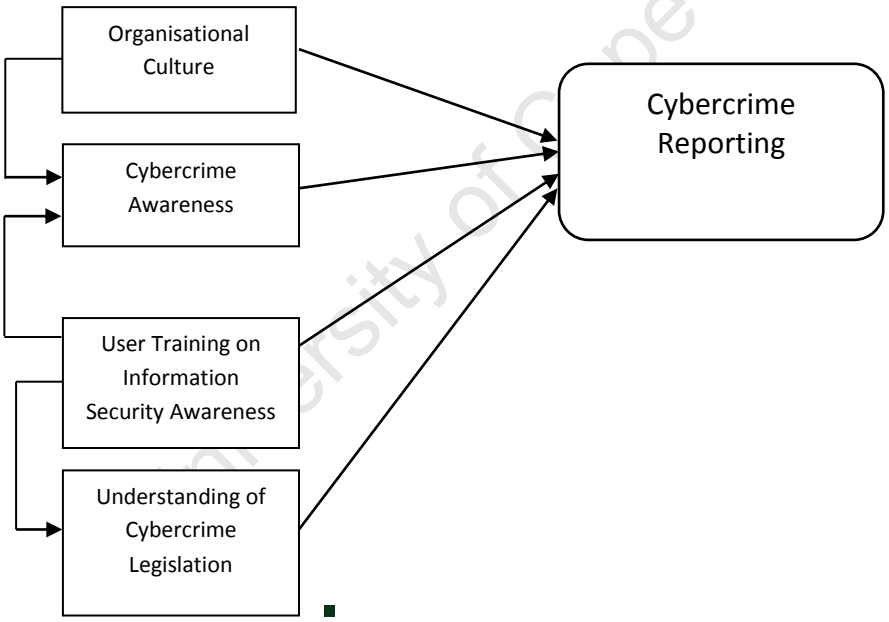

Figure 7: Proposed Framework

3.2 Research Questions

To enable the research to achieve its objectives the following question was used to direct the flow:

- What are the factors that affect the ability for users to report attacks from cybercrime in the public sector in Botswana?

This was the main question, and in order to address it efficiently, it was divided into further sub questions that were meant to help answering it as follows:

(a) How does the organisational culture of the Botswana public sector affect the ability for users to report attacks from cybercrime?
(b) How does cybercrime awareness affect the ability for users to report attacks from cybercrime in the public sector in Botswana?
(c) How does user training on information security awareness affect:
    - cybercrime awareness,
    - understanding of cybercrime legislation
    - the ability for users to report attacks from cybercrime in the Botswana public sector?
(d) How does understanding of the cybercrime legislation of Botswana affect the ability for users to report attacks from cybercrime in the public sector in Botswana?

3.3 Refined Research Objectives

This research will have the following objectives which have been produced based on the focus ideas that were drawn from the literature:

1. To determine the impact of cybercrime awareness on the ability for users to report attacks from cybercrime within the Botswana public sector.
2. To determine the impact of understanding of Botswana Cybercrime Legislation on the ability for users to report attacks from cybercrime within the Botswana public sector.
3. To determine the impact of organisational culture on cybercrime awareness and also on the ability for users to report attacks from cybercrime within the Botswana public sector.
4. To determine how user training on information security awareness impact on cybercrime awareness, understanding of cybercrime legislation, and also on the ability for users to report attacks from cybercrime within the Botswana public sector.

3.4 Development of Hypotheses

Based on the above objectives the following research hypotheses have been developed.

3.4.1 Organisational Culture hypothesis

According to Bluedorn and Lundgren (1993) organisational culture within the public sector needs to be well understood since research has shown that culture plays a very critical role in achievement of goals. It has also been pointed out that the security of every system is dependent upon the security culture that is shared by the employees (IAEA, 2008). Hence the following hypothesis:

H_1: *Organisational Culture has a positive effect on the Ability to Report cybercrime attacks within the public sector organisation*

Schein (1985) has reported that organisational culture has an influence on how employees behave which affects operations within the workplace. Burnes, Cooper and West (2003) also pointed out that employees use the organisational culture to choose their attitudes and behaviour in the workplace. Hence the following hypothesis:

H_2: *Organisational Culture has a positive effect on Awareness of cybercrime within the public sector organisation.*

3.4.2 Cybercrime Awareness hypothesis

A recent research by QinetiQ has shown that no matter how comprehensive and strong the security system for an organisation is, its determinant for success is mainly the awareness level of its employees (Malcolmson, 2009). Furthermore, Arpana and Chauhan (2012) showed that there is general lack of cybercrime awareness by system users of different positions within organisations which contributes to less security breaches in the organisation being reported. Thus the following hypothesis is suggested.

H_3: *Cybercrime Awareness has a positive effect on the Ability to Report attacks from cybercrime within public sector organisation*

3.4.3 User Training (on Information Security Awareness) hypothesis

Studies have shown that while organisations are expanding their technology to be advanced, on the other hand cyber attackers are also looking for easier ways to penetrate this technology by exploiting uneducated computer users who are the weakest link in the system (Whitman & Mattord, 2007; Veerasamy & Taute, 2009). Aloul (2010) notes that mistakes by computer users form part of the top threats to system security for most organisations; he then empirically shows that users in private or government organisations need awareness programs to educate them. Aloul (2010) further states that to enable system users to have a better knowledge of the cybercrime legislation in their countries, these laws should be incorporated as components into existing information security programmes.

Therefore, the hypotheses are suggested as:

H_4: *User Training on Information Security Awareness has a positive effect on Cybercrime Awareness.*

H_5: *User Training on Information Security Awareness has a positive effect on Understanding of Cybercrime Legislation.*

H_6: *User Training on Information Security Awareness has a positive effect on the Ability to Report cybercrime attacks within the public sector organisation.*

3.4.4 Understanding of Cybercrime Legislation hypothesis

Ngakaagae (2010) identified challenges by both the law enforcement agencies, prosecutors and the general public to understand the law related to cybercrime as one of the impediments that hinder proper handling of cybercrime incidents and cases. Nyanda (2010) also reiterated the fact that a lack of understanding of the computer crime law hindered the police and government to fully control cybercrime.

Hence the following hypothesis is suggested:

H_7: *Understanding of Cybercrime Legislation has a positive effect on the Ability to Report cybercrime attacks within the public sector organisation.*

3.5 Summary of Hypotheses

The following summary of hypotheses for the study has been developed based on the discussion from the literature.

H_1: *Organisational Culture has a positive effect on the ability to Report attacks from cybercrime within a public sector.*

H_2: *Organisational Culture has a positive effect on Awareness of cybercrime within the public sector.*

H_3: *Cybercrime Awareness has a positive effect on the Ability to Report cybercrime attacks within the public sector organisation.*

H_4: *User Training on Information Security Awareness has a positive effect on Cybercrime Awareness.*

H_5: *User Training on Information Security Awareness has a positive effect on Understanding of Cybercrime Legislation.*

H_6: *User Training on Information Security Awareness has a positive effect on the Ability to Report cybercrime attacks within the public sector organisation.*

H_7: *Understanding of Cybercrime Legislation has a positive effect on the Ability to Report cybercrime attacks within the public sector organisation.*

The above research hypotheses are summarised in Figure 8 below.

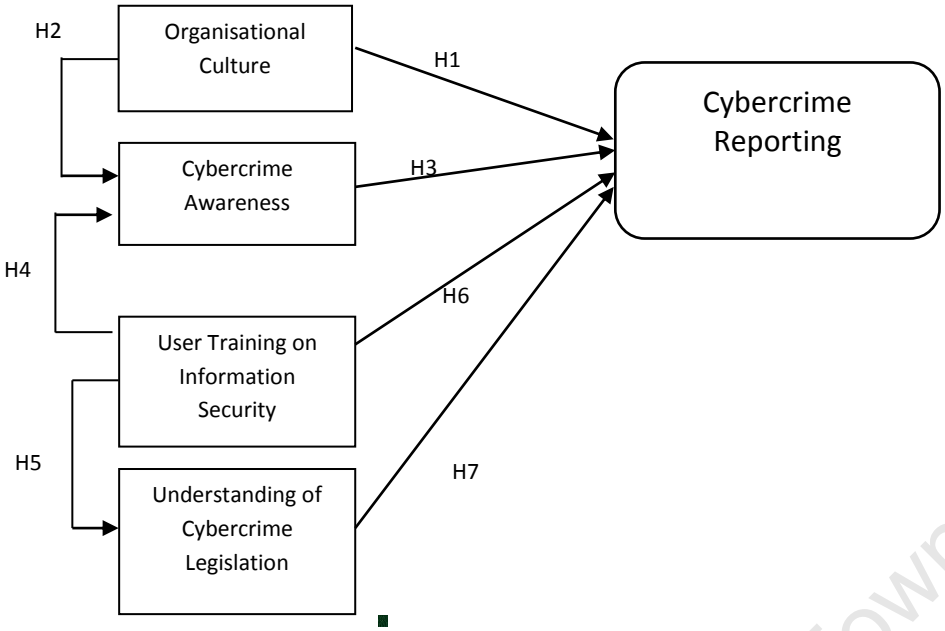

Figure 8: Research Framework with Hypotheses

Chapter 4: Research Methodology

In this section an illustration of how the research was conducted will be provided.

4.1 Research Purpose

This research's purpose is exploratory in nature since it involves testing of hypothesis with an aim to explain how constructs of the developed framework (Cybercrime Awareness; understanding of cybercrime legislation; organisational culture and user training on information security awareness) impact on the ability to report cybercrime attacks within the Botswana public sector. This was achieved by collecting data that was gathered across different government ministries. Thereafter, in order to classify how the different constructs of the framework influenced awareness and reporting of cybercrime, the relationship strength among the constructs was assessed. The research also draws from an existing body of knowledge that other researchers have investigated.

4.2 Research Paradigm and Approach to Theory

The underlying philosophy for this research is positivistic and quantitative in nature. Positivism was chosen because it works better where there is a scientific theory, and empirical data is available to test and falsify the hypotheses. When there are no contradictions that are found during testing then the theory can safely be accepted (Association for Information Systems, 2010). The study is quantitative in nature since this can better provide the data in numbers to represent values of the theoretical constructs that are required to test the hypotheses in order to provide strong scientific evidence of how the hypotheses work (Association for Information Systems, 2010). Therefore, this approach is deemed as most appropriate for this study since it will help to explain how the constructs impact on cybercrime awareness and reporting. Furthermore, results from quantitative studies can easily be generalised to the total population (Arpana & Chauhan, 2012).

The research adopted a deductive approach since the developed framework was formulated with the help from literature (Saunders et al., 1997). Through a deductive position it was easy to test the framework using the quantitative data that was gathered from the questionnaires; this enabled the study to identify patterns that appear across different ministries which have an impact on the awareness and reporting of cybercrime.

4.3 Sampling Plan

Selection of participants should be carefully considered while designing the study in order to ensure that they represent the population well. The selection is normally influenced by the nature of the study itself, hence the selected participants should show key traits possessed by the general population (Bonebright, Miner, Goldsmith & Caudell, 2005).

This study targeted government employees in the Republic of Botswana as its population. To draw the relevant sample a stratified sample approach was employed to obtain a representative sample from the population. The fourteen different government ministries were targeted to be included; and from each ministry the following departments: IT, Human Resource (HR), top management or heads of department, and lastly general computer users (regardless of their department) were included. Another study on cybercrime awareness in India also included senior managers and IT administrators in its sample (Arpana & Chauhan, 2012).

To decide which departments to include in the study purposive sampling was used; IT was chosen because of its involvement with day to day computer systems; while HR was included because it handles all the procedures and functions that deal with staff recruitment and training on different programs that have to be known by government employees; top management were included because of their leading roles in management of their respective departments or ministries; and general computer users were chosen in order to give a perspective of an average computer user regarding cybercrime awareness and reporting. The sample was also limited to the capital city, Gaborone since that is where all the ministries' headquarters are located. Moloi and Mutula (2007) conducted a similar study on e-government in Botswana and also restricted their sample to Gaborone for the same reasons.

In order to reduce errors for the study estimates and also to guarantee a good sample size for strata, a stratified sample was used. To achieve this, the study aimed to include 5 participants from the 4 categories or strata that were identified from each ministry; making it a total of 20 participants per ministry, and 260 from the 14 ministries. This figure was chosen bearing in mind that it is always a challenge to have enough responses from government employees (Moloi & Mutula, 2007).

Roscoe (1975) advised that a sample size larger than 30 and less than 500 is enough for quantitative study; it provides a sufficient sample size which is conducive to give accuracy in statistical analysis (Leedy & Ormrod 2005. The aim was to gather a total of at least 50 responses which is deemed acceptable for quantitative analysis (Lucas, 1991). Another quantitative study by Ali and Green (2007) used about 54 responses to conduct its analysis, and this was found to be sufficient enough. However, this study was able to receive 54 valid responses that were used in the analysis.

All government ministries were included in this study in order to provide results that can be generalised for the whole public sector (Moloi & Mutula, 2007). Through e-Government initiatives all ministries in Botswana public sector are now making uses of ICT at most levels of their operations and are also connected to the Internet. Therefore, there is a reasonable need for protecting their data and services from being affected by cybercrime.

For demographic attributes such as age and gender the study did not have any specific requirements but just adopted the Botswana public sector age range of 21 to 65 years, both female and male.

4.4 Questionnaire Design

4.4.1 Overview of the Questionnaire

Due to the nature of the study being exploratory, literature on this subject was used as the basis to develop questions that were used for the study. Generating research questions from literature has been used in other similar studies (Arpana & Chauhan, 2012).

4.4.2 Questionnaire Structure & Content

The questionnaire used in the study had three main sections. The first one requested the respondents to provide demographic data that was deemed non-sensitive, such as Ministry Name, Department, Gender, Age Group (select from given options), Nationality and Experience using computers (given as final question in questionnaire). The second section comprised of the actual questions of the survey questionnaire grouped according to their constructs.

The survey had a total of 23 questions that were separated into five categories. The first category was called ‘Awareness’ and it had 4 questions; followed by ‘Cybercrime

Legislation' with four questions as well; 'Organisational Culture' was next with five question; then 'Information Security Training' followed with five question; while the last category was named 'Cybercrime Reporting' which also had five questions. The final section in the survey was an extra space provided for additional comments that the respondents might have wanted to make in relation to the study.

4.4.3 Questionnaire Items

The responses received from the survey results were used to attempt to find answers to the following research questions that were outlined in section 3.2 above:

(a) How does the organisational culture of the Botswana public sector affect the ability for users to report attacks from cybercrime?

(b) How does cybercrime awareness affect the ability for users to report attacks from cybercrime in the public sector in Botswana?

(c) How does user training on information security awareness affect:

- cybercrime awareness,
- understanding of cybercrime legislation
- the ability for users to report attacks from cybercrime in the Botswana public sector?

(d) How does understanding of the cybercrime legislation of Botswana affect the ability for users to report attacks from cybercrime in the public sector in Botswana?

In order to answer the above four questions, hypotheses that were presented in section 3.5 previously were tested. Table 6 shows the constructs together with their questionnaire items.

Construct	Instrument Items
Cybercrime Awareness (AWARENESS)	1. I understand what cybercrime is 2. I can identify cybercrime incidents/attacks 3. I know how to protect myself from cybercrime 4. I understand the impact of cybercrime to my organisation
Understanding of Cybercrime Legislation (LEGISLATION)	5. I know about the cybercrime law of Botswana (Cybercrime & Computer Related Crimes Act). 6. I know the contents of the cybercrime law of Botswana 7. My organisation makes its employees aware of the cybercrime law 8. I know that the cybercrime law is helpful to address cybercrime in my organisation
Organisational Culture (O_CULTURE)	9. My organisation makes it easy for the staff members to report any issues of concern 10. My organisation mostly informs all employees about critical or important information 11. Employees are free to report their issues of concern to anyone regardless of position in the organisation 12. My organisation provides general induction (training) to new employees 13. Employees normally share information on critical issues in my organisation
User Training on Information Security Awareness (TRAINING)	14. My organisation has an information security awareness training programme 15. IT officers in my organisation are trained on how to respond to information security matters 16. My organisation provides ongoing refresher courses/training on information security 17. Training on information security awareness is important for my organisation 18. Most employees (who use computers) in my organisation have received information security awareness training
Cybercrime Reporting (REPORTING)	19. I always report cybercrime incidents that I experience 20. I know where to report cybercrime incidents in my organisation 21. The IT department/unit in my organisation understands what to do about reported cybercrime incidents 22. I think most cybercrime incidents are reported in my organisation 23. I know that it is important to report cybercrime incidents in my organisation

Table 7: Constructs and Instrument items

The questionnaire was measured using a five-point Likert scale with anchors from 1-5 (1-Not at all, 2-Little, 3-Average, 4-More than average, & 5-A lot); and respondents selected the answers by ticking or crossing out their choice. This was deemed suitable for this study since it was expected that most of participants would be lacking knowledge regarding the cybercrime area. Therefore, having a Likert scale (with its odd numbers) would not compel participants to make a selection that they were uncertain on how to rate it (Ghauri & Gronhaug, 2002). The research questionnaire is contained in Appendix C.

4.4.4 Pilot Study

The first developed version of the research instrument was evaluated to test its validity with the help of three (fellow students) colleagues, a researcher and senior lecturer from the University of Cape Town. Their feedback was used to adjust the research instrument to be relevant for the study. Significant adjustments made included rephrasing some questions to make them suitable for the target sample by making them less technical in nature. To verify

that the research instrument would give reliable and accurate results needed for analysis, a pilot study was carried out using convenience sampling. The Botswana Consulate General office in Cape Town was requested to help with piloting the research instrument, where seven people volunteered to complete all of the questions. From this pilot study, it was recommended by the participants that the order of questions should be altered in order to have less difficult questions appear at the beginning and difficult ones to follow later on so that respondents feel comfortable to answer the questions. The advice and recommendations that were gathered while testing the research instruments were incorporated into the research instrument in consultation with the research supervisor.

4.5 Data Collection Method

4.5.1 Data Collection Permission

As already stated in section 4.3, the sample for this study was limited to Botswana government employees in the capital Gaborone, hence to collect the data a survey strategy was used to enable the researcher to reach the fourteen ministries.

The researcher first had to seek a written permission from the government research unit that was to be presented to each ministry as proof of authorisation to conduct the study. Furthermore, permission had to be sought out at each ministry before data collection could commence and failure to get this meant that the affected ministries were left out of the study.

4.5.2 Quantitative Data Collection

To distribute the survey questionnaires in each ministry different methods suitable for each type of respondents was used. For senior management, the questionnaires were given to their secretaries to arrange a suitable time for them to complete. For the IT and HR unit, the questionnaires were given to the unit heads to identify the people who would complete them. To reach the 'general computer users' category the researchers requested the IT unit to distribute the questionnaires to any five people to complete them. The respondents were asked to answer all the questions for their responses to be meaningful to the study; it took about 5-10 minutes to complete the questionnaire. The questionnaires were normally administered by the researcher and collected immediately. Where it was impossible to do this they were left at the ministries and collected within 2-3 working days in order to give respondents time to complete them. This exercise was repeated at all the different ministries in order to complete the data collection.

The first round of data collection did not yield much fruits since some of the respondents who had remained with the questionnaires reported that they had misplaced the questionnaires, hence this delayed the process since a new set of questionnaires had to be handed out again for replacement. This problem was experienced in a number of ministries.

4.6 Data Analysis Techniques

4.6.1 Quantitative Data Analysis

After collecting data that has to be analysed in a quantitative manner, it has to be captured and prepared in a format that allows relevant tests to do conducted on it (Cavana et al., 2001). To achieve this, a spreadsheet software (MS Office Excel 2010) was used to capture all usable responses gathered from the questionnaire; a total of 54 responses were received. Thereafter, the captured data was exported to a statistical analysis software (Statistica 10) for further in-depth analysis of the data to test the hypotheses for the research.

The following statistical tests were conducted on the data for analysis:

- **Descriptive Statistics**: this was conducted in order to describe respondents' profile and also to obtain their level of computer knowledge. Mean values were also obtained for key variables in the research framework. To determine the dispersion of data and also the standard deviation, Variance statistics was employed.

- **Graphical Representation**: a spreadsheet software (MS Office Excel 2010) was used to produce the necessary pie charts and bar charts in order to display summaries from the raw data before any analysis was conducted.

- **Factor Analysis**: the questionnaire items were analysed using Exploratory Factor Analysis (EFA) in order to determine whether they would group into distinctive factors; this further checked the constructs for validity.

- Item Analysis using **Cronbach's Alpha** (α): this provided tests that checked the research constructs for internal consistency and reliability.

- **Spearman's correlation rank coefficient** (r): this was helpful to establish whether there were any relationships between constructs and also how strong they were.

- The final tests were **Multiple Linear Regression Analyses**; these were conducted on the hypotheses in order to obtain the regression values for the linear equations that were formulated to test how the hypotheses for the research framework impacted on each other, to determine whether this would increase the variance explained in the dependent variables.

4.7 Key Assumptions

The key assumptions for the research were as follows:

- Cybercrime is not currently managed properly in the Botswana public sector.
- The necessary permission would be granted by the Botswana government for the researcher to conduct the study.
- The study would have enough participants to enable it to meet the necessary data requirements for analysis.
- The developed research framework would contribute greatly to the Botswana government by providing an effective tool to help in improving awareness and reporting of cybercrime attacks in the public sector.

4.8 Data Integrity and Ethical Considerations

The researcher submitted all documents that would be used for this research (survey questionnaire and research cover letter) to the Ethics Committee of the Department of Information Systems at the University of Cape Town for approval in order to verify that they adhere to ethical requirements. Furthermore, the researcher had to resubmit the research instruments to the Botswana government research unit for ethical and integrity approval before permission could be given to conduct the research. During the research all participants were given the relevant research instrument to read beforehand and also the researcher verbally explained the purpose of the research for them to choose whether to participate or not.

To protect the identity of all respondents, the researcher made sure that personal identity was kept anonymous throughout the study. To achieve this there was no personal or sensitive information that was gathered by the research instruments. Upon collection of the completed questionnaires to ensure data integrity and quality, they were all checked to verify that they have been properly completed and contained nothing irregular.

4.9 Research Timeframe

The research was carried out from mid-March 2012 to end of April, and took about a month and half to complete. This took a considerable time to do due to the fact that the researcher had to travel between Cape Town (South Africa) and Gaborone (Botswana) where the research was conducted. Furthermore permission had to be sought from the Botswana Government before commencing with the research. Therefore strict time constraints were imposed by the duration needed to complete the study which meant that a cross-sectional timeline had to be used.

Chapter 5: Descriptive Statistics

5.1 Introduction

This chapter presents the demographic profile of the respondents that was obtained from the survey; it was obtained from the first part (Demographics) and also the last question of the questionnaire. In this section important patterns that have been identified from the sample are presented. Therefore it will give an outline of the descriptive statistics for items and constructs that were used in the questionnaire.

5.2 Sample Survey Profile

5.2.1 Ministry

The number of ministries that took part in the survey was 10 out of the 14 ministries in the government. This number is a fair representation of the government sector given that only a few did not participate. Those that have not been included did not participate due to the fact that they did not respond to the survey questionnaire which was given to them. The highest number of responses was 11, received from the ministry of State President; two other ministries also showed good responses of nine by Health, and eight from Defence, Justice & Security. The lowest responses came from two ministries of Foreign Affairs and Local Government with two responses from each. This data is illustrated below in Figure 9.

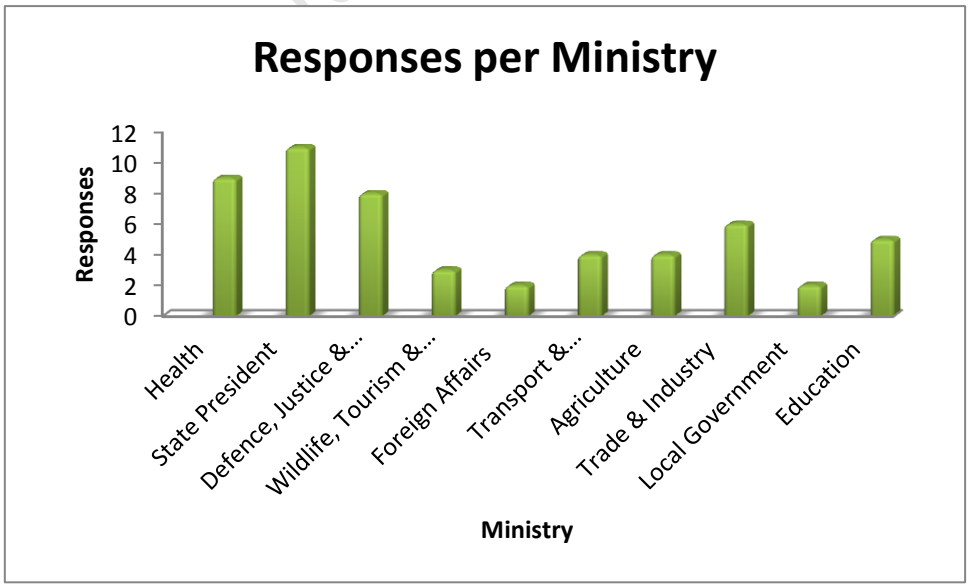

Figure 9: Responses per Ministry

5.2.2 Department

For this survey the target departments or units that were included for study are: IT; Human Resources; top management (grouped under Corporate Services) and other general computer users from any other department, these were classified under Users. The respondents from IT were 18, representing the majority of participants. Corporate Services had 10 respondents, while Human Resources had 15 respondents and lastly 11 from the User category. Human Resources had the second largest representation of respondents; however all the departments seem to have been fairly represented in the survey as shown in Figure 10 below.

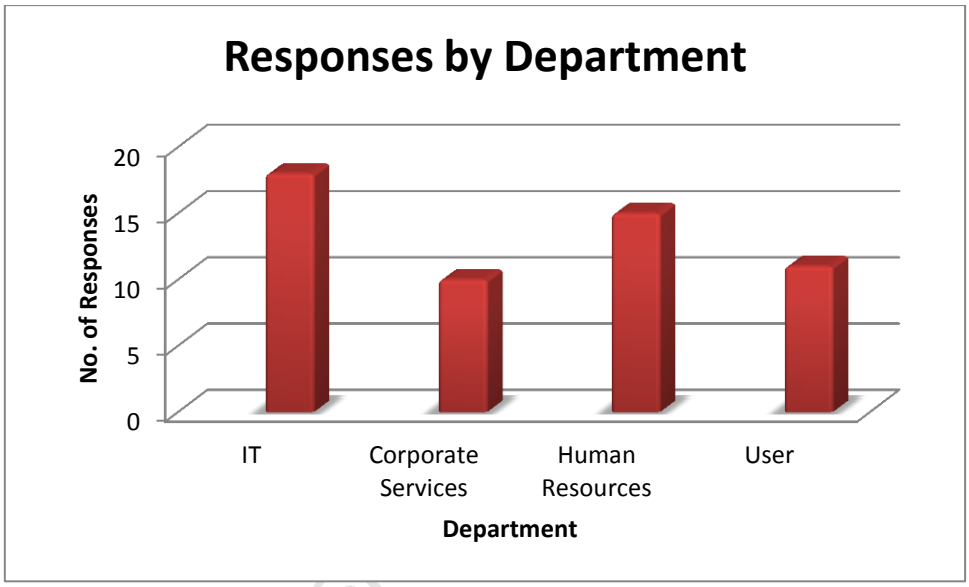

Figure 10: Department of Respondents

5.2.3 Gender

All respondents were encouraged to fill out every section of the questionnaire in order for their responses to be used in the study; therefore this resulted in participants indicating their gender as well. This is illustrated in Figure 11 showing gender distribution by respondents.

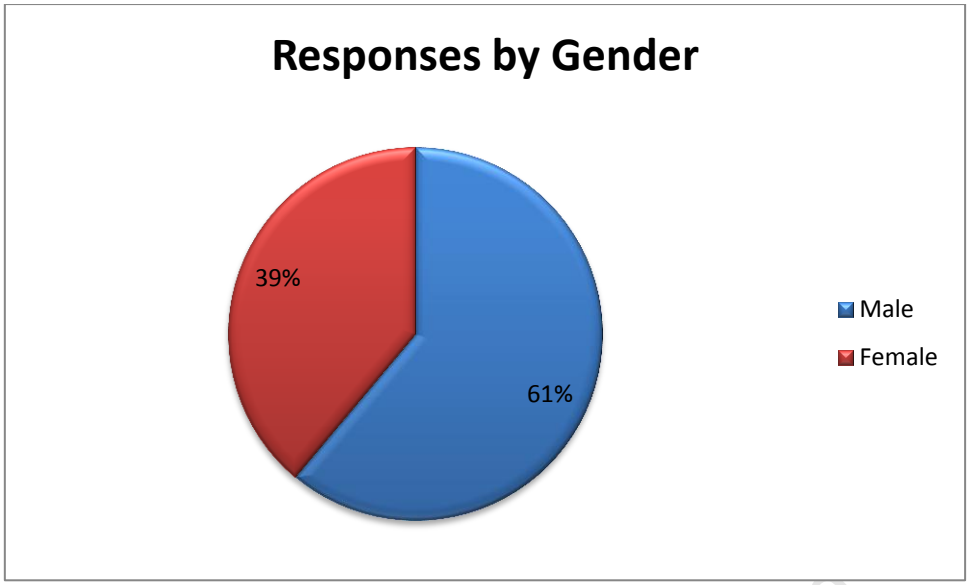

Figure 11: Gender of Respondents

The distribution of gender for respondents shows that more males participated in the survey than females, 61% and 39% respectively. The number of females that participated is however good for the sample, since it can be rounded off to 40%. The dominance by males could be because there are more males than females employed in the IT sector, which also had more participants as compared to other departments as shown in Figure 10.

5.2.4 Age

Age distribution for the participants was dominated more by the 21 to 34 age group which accounted for 59% of the respondents. This was partly influenced by the fact that this group is still young and mostly comfortable to participate in a computer related survey; hence elderly employees would insist on younger employees to participate. 33% of respondents were from the 35 to 44 age group which also comprise relatively younger employees. The remaining 8% was made up of people from the 45 to 54 age group. The last two age groups of 55 to 64 and 65 and above were not represented in the survey. These age groups are illustrated in Figure 12.

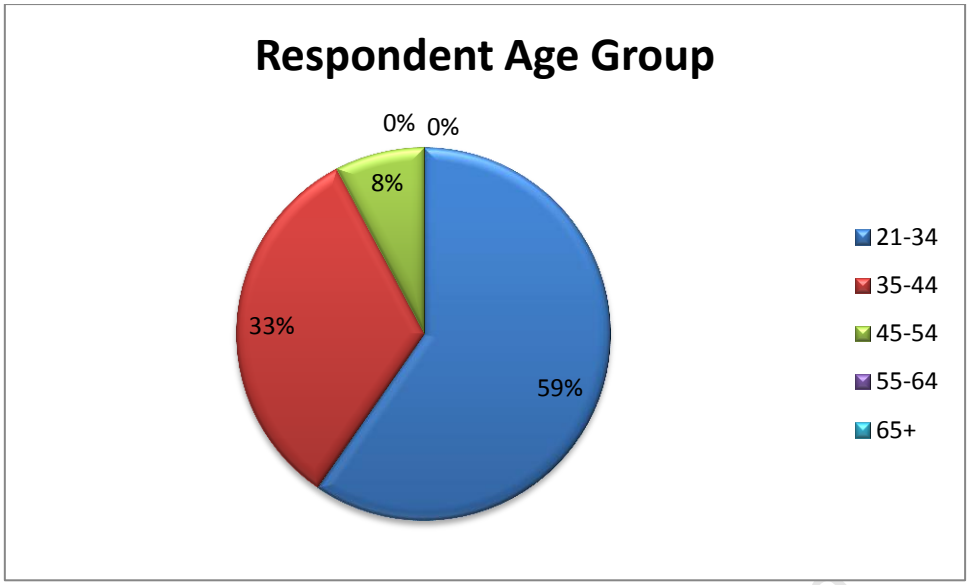

Figure 12: Respondents Age Group

5.2.5 Nationality

All of the respondents that participated in this survey indicated that they were Batswana (citizens of Botswana). Therefore, results of the survey would be 100% from Botswana citizen government employees from the participating ministries.

5.2.6 Experience in computer use

Figure 13 shows that most respondents had the necessary experience required to use computers efficiently. 41% responded that they possessed excellent skills; while 39% had indicated that their skills were very good. The remaining 20% the surveyed sample showed that 18% had only average skills, while 2% had little experience with computer use. Therefore, the results indicate that majority of respondents (80%) had proficient knowledge on how to use computers.

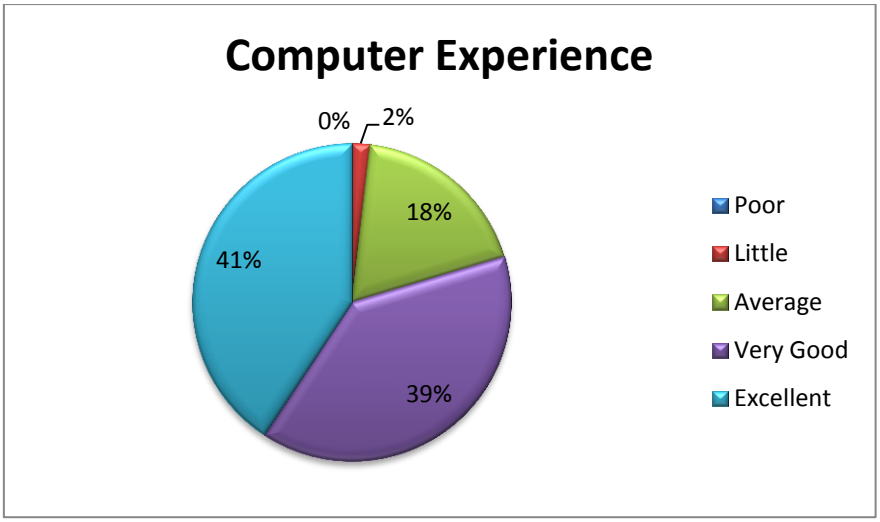

Figure 13: Respondent Computer Experience

5.3 Questionnaire Items Descriptive Statistics

This section presents the descriptive statistics that were conducted for the questionnaire items; more detailed results for this breakdown are included in Appendix D. The codes that were used for each questionnaire item are illustrated in Table 8.

Code	Questionnaire Item	Code	Questionnaire Item
AWARE1	1. I understand what cybercrime is	CULTR5	13. Employees normally share information on critical issues in my organisation
AWARE2	2. I can identify cybercrime incidents/attacks	TRAIN1	14. My organisation has an information security awareness training programme
AWARE3	3. I know how to protect myself from cybercrime	TRAIN2	15.IT officers in my organisation are trained on how to respond to information security matters
AWARE4	4. I understand the impact of cybercrime to my organisation	TRAIN3	16.My organisation provides ongoing refresher courses/training on information security
LEGIS1	5. I know about the cybercrime law of Botswana (Cybercrime & Computer Related Crimes Act).	TRAIN4	17. Training on information security awareness is important for my organisation
LEGIS2	6. I know the contents of the cybercrime law of Botswana	TRAIN5	18. Most employees (who use computers) in my organisation have received information security awareness training
LEGIS3	7. My organisation makes its employees aware of the cybercrime law	REPOT1	19. I always report cybercrime incidents that I experience
LEGIS4	8. I know that the cybercrime law is helpful to address cybercrime in my organisation	REPOT2	20. I know where to report cybercrime incidents in my organisation
CULTR1	9. My organisation makes it easy for the staff members to report any issues of concern	REPOT3	21. The IT department/unit in my organisation understands what to do about reported cybercrime incidents
CULTR2	10. My organisation mostly informs all employees about critical or important information	REPOT4	22. I think most cybercrime incidents are reported in my organisation
CULTR3	11. Employees are free to report their issues of concern to anyone regardless of position in the organisation	REPOT5	23. I know that it is important to report cybercrime incidents in my organisation
CULTR4	12. My organisation provides general induction (training) to new employees		

Table 8: Questionnaire Item Codes

Results for descriptive statistics that were performed for the questionnaire items showed that the item with the highest mean value was Item 11 (CULTR3) with (4.13) on the other hand the lowest meant was Item 23 (REPOT5) with (1.37). The Implications for this is that Item 11 (CULTR3) had responses ranging between 'More than average' and 'A lot' on the Likert scale, while Item 23 (REPOT5) had responses between 'Not at all' and 'Little'. The mean scores for all other items were generally very low with score below 2. The only exception was with Organisational Culture items which scored between 2.43 and 4.13 on the 5 Likert scale.

Chapter 6: Reliability & Validity Testing

To ensure that the data is suitable for use in any significant statistical tests, it needs to be tested for reliability and validity. This is provided below.

6.1 Testing for Reliability

To establish the reliability and quality of constructs and variables used in the research instrument, Brown and Jayakody (2008) advice that the instrument should be checked for internal consistency. To achieve this Cronbach's Alpha denoted by 'α' (coefficient alpha) is commonly used to point out the correlation between items in one set (Brown & Jayakody, 2008; Molla, 2001). An alpha threshold value of 0.80 for Cronbach Alpha is recommended although other authors (Nunnally, 1978; Fornell & Larcker, 1981; Hair, Black, Babin, Anderson & Tatham, 2006) advice that for exploratory studies the threshold can be set to 0.60 even though it is ideal to have a value that is more than 0.70 for a higher reliability for items in a construct (Tan & Teo, 2000).

In addition an item analysis was performed on the items in each construct. According to Hart, Esat, Rocha and Khatieb (2007) to conduct an item analysis a construct should contain at least three items (questions) in it, and this was met by all constructs in this study. All of the five constructs showed to have very strong correlation between their items (questions), with Organisational Culture (O_Culture) showing the lowest Cronbach Alpha (α) value of 0.63. Three constructs (Awareness, Legislation and Training) loaded up 'α' values greater than 0.8 while one (Reporting) loaded α value of 0.76. This showed that their items are strongly reliable and acceptable for use in further statistical analysis. A summary of these results is shown below in Table 8, while the full result can be found in Appendix F.

Construct Full Name	Construct Identity	Items	Cronbach (α)
Cybercrime Awareness	Awareness	4	0.83
Understanding of Cybercrime Legislation	Legislation	4	0.83
Organisational Culture	O_Culture	5	0.63
Information Security Training	Training	5	0.84
Cybercrime Reporting	Reporting	5	0.76

Table 9: Item Analysis Results Summary

6.2 Validity Testing

The researcher conducted factor analysis on the data that was received from respondents. This was done in order to observe what patterns would emerge from the variables to show whether any factors could be generated efficiently without losing much information (Hair, Black, Babin & Anderson, 2006). Two types of factor analysis are outlined in DeCoster (1998) as Exploratory, which seeks to identify underlying constructs that influenced responses; and Confirmatory, which focus on whether responses are influenced by constructs in a specific manner. This research adopted the exploratory factor analysis since it was found suitable to test the constructs' validity. Furthermore confirmatory factor analysis has been reported to be restrictive in nature while exploratory is not and also is more used than confirmatory (Peterson, 2000).

Peterson (2000) states that the goal of factor analysis is achieved when the number of items that convey the defined constructs has been fully or partially extracted from the data; this will show that the construct is valid. The loading of the factors represent how the variables and factors correspond to one another (Hair, Black, Babin, Anderson & Tatham, 2006). There seems to be no general stated rule for choosing the threshold for factor loading, however as 'a rule of thumb' 0.50 is normally accepted (Merenda, 1997). Other authors state different thresholds for determining factor loadings due to lack of consensus on this issue; Hair, Anderson, Tatham & Black (1998) note that factor loading of more than 0.30 meets the minimal requirement, 0.40 are more important, while loadings of 0.50 and above are more significant.

The researcher conducted exploratory factor analysis on all variables with the following criteria:

- Threshold value : > 0.55
- Rotation Method : Varimax Normalised
- Minimum eigenvalue : 1.000
- Maximum factors : 5

The summary for results of the factor analysis is presented in Table 9 below, while full results can be found in Appendix E. These results show that most of the items appeared

generally well in factors matching their expected constructs; they also loaded with values greater than 0.60 except for only one item under factor 1.

However, two constructs did not manage to have all of their items loading up in the factors. These were Organisational Culture (Factor 5) where the first and last items did not load up at all, (CULTR1 and CULTR5); and User Training on Information Security Awareness (Factor 4) with the last item (TRAIN 5) not loading up as well.

Generally as already mentioned about, most items loaded with values greater than 0.60 in all constructs and factors, except for only a few items as identified above. Therefore, the results from the exploratory factor analysis show acceptable validity for the constructs of the research instrument.

Factor Loadings (Varimax normalized) Extraction: Principal components (Marked loadings are >.550000)					
	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
AWARE1		0.842051			
AWARE2		0.863327			
AWARE3		0.769254			
AWARE4		0.680171			
LEGIS1			0.819750		
LEGIS2			0.695558		
LEGIS3			0.783965		
LEGIS4			0.839818		
CULTR1					
CULTR2					0.615359
CULTR3					0.809004
CULTR4					0.785897
CULTR5					
TRAIN1				0.791371	
TRAIN2				0.832947	
TRAIN3				0.867555	
TRAIN4				0.701890	
TRAIN5					
REPOT1	0.831764				
REPOT2	0.795239				
REPOT3	0.701893				
REPOT4	0.566906				
REPOT5	0.607170				

Table 10: Exploratory Factor Analysis Results

6.3 Eigenvalue Analysis

Hart et al. (2007) states that the purpose of the Eignvalue analysis is to show how much each factor explains the variance which is accumulated for the whole questionnaire items. Results of the Eignvalues for this study based on the 23 items from the questionnaire that loaded into 5 factors accounted for a cumulative variance value of 62.6%, which for an initial study presents fairly acceptable overall construct validity. Table 10 below shows the results of the Eigenvalue analysis.

	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative (%)
Factor 1	4.554872	19.80379	4.55487	19.80379
Factor 2	3.035866	13.19942	7.59074	33.00321
Factor 3	2.842333	12.35797	10.43307	45.36118
Factor 4	2.108933	9.16927	12.54200	54.53045
Factor 5	1.852229	8.05317	14.39423	62.58362

Table 11: Eigenvalue Analysis Results

Chapter 7: Results and Discussion

This chapter presents the tests that were carried out on the hypotheses that were presented in section 3.5; this was done in two phases. The first test was a Correlation Analysis that was carried out using Spearman Ranking Correlation, while the other one was an analysis done with the help of a Multiple Regression technique. These two tests are elaborated further on in the following sub sections.

7.1 Correlation Analysis

The correlation analysis was conducted on all five constructs of the research framework that was developed for this study in order to determine the strength of relationships. These constructs were presented as follows: Cybercrime Awareness (AWARENESS), Understanding of Cybercrime Legislation (LEGISLATION), Organisational Culture (O_CULTURE), User Training on Information Security Awareness (TRAINING) and finally Cybercrime Reporting (REPORTING). The correlations between these constructs were established by using non-parametric testing called Spearman Rank Correlation. This test was used because of two reasons; the first being that it is suitable to handle sample data that was derived by means of a Likert scale (e.g. with ranking from 1 – 5), and secondly it does not need any assumption on the distribution for the sample (Hart et al., 2007). The results of this test are illustrated by the correlation matrix in Table 11 below.

Variable	Spearman Rank Order Correlations (All_Constructs) MD pairwise deleted Marked correlations are significant at p <.05000				
	AWARENESS	LEGISLATION	O_CULTURE	TRAINING	REPORTING
AWARENESS	1.000000				
LEGISLATION	-0.014699	1.000000			
O_CULTURE	0.269948	-0.018398	1.000000		
TRAINING	0.352139	0.222157	0.133159	1.000000	
REPORTING	0.407346	0.291043	0.096934	0.424312	1.000000

Table 12: Correlation Analysis Results

The correlation matrix from Table 11 above shows that most the constructs that were associated with each other in the Cybercrime Reporting framework in Section 3.5 have a significant positive correlation with one another at 5% significance level ($p<0.05$); only two constructs from the research framework that were expected to be significantly positively

correlated failed to show this relationship. These are Cybercrime Legislation (LEGISLATION) and Information Security Training (TRAINING) which showed a non-significant positive correlation (r=0.22). The other pair of constructs was between Cybercrime Reporting (REPORTING) and Organisational Culture (O_CULTURE) that yielded an insignificant correlation value (r=0.10). The positively significantly correlated constructs had the following correlation values: Cybercrime Awareness (AWARENESS) and Organisational Culture (O_CULTURE) was (r=0.27); Cybercrime Awareness (AWARENESS) and Information Security Training (TRAINING) was (r=0.35); Cybercrime Reporting (REPORTING) and Cybercrime Awareness (AWARENESS) was (r=0.41); Cybercrime Reporting (REPORTING) and Cybercrime Legislation (LEGISLATION) was (r=0.29); and finally Cybercrime Reporting (REPORTING) and Information Security Training (TRAINING) was (r=0.42) which also showed the strongest correlation.

To show the relationship for hypotheses in the research framework, their correlation analysis summary is presented below in Table 12.

Hypotheses	Constructs tested	Correlation Value (r value)	Relationship
H_1	REPORTING vs. O_CULTURE	0.10	Non-significant
H_2	AWARENESS vs. O_CULTURE	0.27	Significant
H_3	REPORTING vs. AWARENESS	0.41	Significant
H_4	AWARENESS vs. TRAINING	0.35	Significant
H_5	LEGISLATION vs. TRAINING	0.22	Non-significant
H_6	REPORTING vs. TRAINING	0.42	Significant
H_7	REPORTING vs. LEGISLATION	0.29	Significant

Table 13: Correlation Analysis Summary

It was interesting to note that most hypotheses from the research framework had a positive significant correlation to one another; this showed that to a certain degree they were related. To help determine the hypotheses that will be accepted or rejected, the following section will subject the variables to further analysis using Multiple Regression.

7.2 Multiple Regression Analysis

To evaluate the association between dependent and independent variables, the hypotheses were further tested using multiple regression analysis (Hair et al., 2006). To achieve this, the

beta value (β) and coefficient of determination (R^2) for each hypothesis relationship is calculated (Van der Heijden, 2003).

Garson (2008) outlines the equation for analysing multiple regression in this format:

$Y_1 = b_1X_1 + b_2X_2 + ... + b_nX_n + c$

The symbols represent:

- Y_1 (dependent variable);
- X_1, X_2, X_n (independent variables);
- b_1, b_2, b_n (regression coefficients for dependent variable Y_1);
- c (constant) which shows what the dependent variable Y_1 is when (X_1, X_2, X_n) independent variables are equal to 0 and the regression line meets with the y axis.

To test the hypotheses associations generated for this research, the multiple regression equations below were formulated:

Equation 1: **REPORTING** = a + h_1 * *O_CULTURE* + h_3 * *AWARENESS* + h_6 * *TRAINING* + h_7 * *LEGISLATION*

Equation 2: **AWARENESS** = b + h_2 * *O_CULTURE* + h_4 * *TRAINING*

Equation 3: **LEGISLATION** = d + h_5 * *TRAINING*

The symbols in the above equations represent the following: h1 to h7 are the beta values (β) for the respective hypotheses while a, b & d are the constants.

7.2.1 Regression Analysis Results for Equation 1

The above equations (1-3) are of the recursive simultaneous model and can be estimated by separate multiple linear regression analysis done on each of them (Pindyck & Rubinfield, 1998). Therefore, hypotheses H_1, H_3, H_6 and H_7, (Equation 1) were first tested. This equation had the following independent variables: Organisational Culture (O_CULTURE), Cybercrime Awareness (AWARENESS), User Training on Information Security Awareness

(TRAINING) and Understanding of Cybercrime Legislation (LEGISLATION), while Cybercrime Reporting (REPORTING) was the dependent variable. Table 14 shows the multiple regression analysis results for Equation 1.

N=54	Regression Summary for Dependent Variable: Reporting (All_Constructs_Responses Cybercrime) R= .56843172 R²= .32311462 Adjusted R²= .26785867 F(4,49)=5.8476 p<.00063 Std.Error of estimate: .41708					
	b*	Std.Err. (of b*)	b	Std.Err. (of b)	t(49)	p-value
Intercept			0.283098	0.305688	0.926102	0.358932
AWARENESS	0.326400	0.130658	0.246943	0.098852	2.498116	0.015890
LEGISLATION	0.259562	0.122113	0.220298	0.103641	2.125590	0.038603
O_CULTURE	-0.006003	0.123640	-0.004882	0.100558	-0.048549	0.961476
TRAINING	0.261037	0.129054	0.235285	0.116323	2.022694	0.048580

Table 14: Equation 1 Regression Analysis Results

The coefficient of determination (R^2) value for the multiple regression model of Equation 1 was 32.31%. This means that 32.31% of the total variation in Cybercrime Reporting (REPORTING) can be explained by the independent variables (Cybercrime Awareness, User Training on Information Security, and Understanding of Cybercrime Legislation). These results are explained more in Section 7.3.

Equation 1 thus becomes:

REPORTING = 0.283 + 0.247 * *AWARENESS* + 0.235 * *TRAINING* + 0.220 * *LEGISLATION*

7.2.2 Regression Analysis Results for Equation 2

Multiple linear regression tests were then performed on Hypotheses H_2 and H_4 (Equation 2). The independent variables for this equation were Organisational Culture (O_CULTURE) and User Training on Information Security (TRAINING), the dependent variable on the other hand was Cybercrime Awareness (AWARENESS). Table 15 shows the results for Equation 2.

N=54	Regression Summary for Dependent Variable: Awareness (All_Constructs_Responses Cybercrime) R= .42470594 R²= .18037513 Adjusted R²= .14823298 F(2,51)=5.6118 p<.00627 Std.Error of estimate: .59461					
	b*	Std.Err. (of b*)	b	Std.Err. (of b)	t(51)	p-value
Intercept			0.430653	0.387490	1.111390	0.271613
O_CULTURE	0.275375	0.127640	0.296030	0.137214	2.157436	0.035706
TRAINING	0.292856	0.127640	0.348899	0.152066	2.294396	0.025918

Table 15: Results for Equation 2 Regression Analysis

Equation 2 had coefficient determination (R^2) value of 18.03% for its multiple regression analysis. This means that 18.03% of the total variation in Cybercrime Awareness (AWARENESS) can be explained by the independent variables (Organisational Culture, and User Training on Information Security).

Equation 2 thus becomes:

AWARENESS = 0.431 + 0.296 * *O_CULTURE* + 0.349 * *TRAINING*

7.2.3 Regression Analysis Results for Equation 3

Multiple linear regression was tested for Equation 3 using Hypotheses H_5. This equation had its independent variable as User Training on Information Security (TRAINING), whilst the dependent variable was Cybercrime Legislation (LEGISLATION). Table 16 shows the results for Equation 3.

N=54	Regression Summary for Dependent Variable: Legislation (All_Constructs_Responses Cybercrime) R= .24299930 R²= .05904866 Adjusted R²= .04095344 F(1,52)=3.2632 p<.07664 Std.Error of estimate: .56243					
	b*	Std.Err. (of b*)	b	Std.Err. (of b)	t(52)	p-value
Intercept			1.131422	0.227546	4.972284	0.000008
Training	0.242999	0.134518	0.258065	0.142858	1.806438	0.076638

Table 16: Results for Equation 3 Regression Analysis

Equation 3 had coefficient determination (R^2) value of 5.90%, which means that 5.90% of observed total variation in Cybercrime Legislation (LEGISLATION) can be explained by the independent variables (User Training on Information Security).

Equation 3 thus becomes:

LEGISLATION = 1.131 + 0.258 * *TRAINING*

7.3 Results of the Hypothesis Testing

Below (Table 17) are the results that were obtained from hypotheses testing in section 7.1 and 7.2 (correlation and multiple regression analysis):

Hypothesis	Independent Variable	Dependent Variable	Beta Value β	p-level (p < 0.05)	Hypothesis Supported
H1	Organisational Culture (O_CULTURE)	Cybercrime Reporting (REPORTING)	-0.004	0.961476	No
H2	Organisational Culture (O_CULTURE)	Cybercrime Awareness (AWARENESS)	0.296	0.035706	***Yes***
H3	Cybercrime Awareness (AWARENESS)	Cybercrime Reporting (REPORTING)	0.247	0.015890	***Yes***
H4	User Training on Information Security Awareness (TRAINING)	Cybercrime Awareness (AWARENESS)	0.349	0.025918	***Yes***
H5	User Training on Information Security Awareness (TRAINING)	Cybercrime Legislation (LEGISLATION)	0.258	0.076638	No
H6	User Training on Information Security Awareness (TRAINING)	Cybercrime Reporting (REPORTING)	0.235	0.048580	***Yes***
H7	Cybercrime Legislation (LEGISLATION)	Cybercrime Reporting (REPORTING)	0.220	0.038603	***Yes***

Table 17: Results of Hypothesis Testing

To give a better understanding of which hypotheses were supported and those that were not, the following table (Table 18) shows a tick (✔) for supported ones and a cross (✘) for those not supported:

Hypothesis	Description	Supported/ Not Supported
H_1	*Organisational Culture has a positive effect on the ability to Report attacks from cybercrime within a public sector organisation.*	✗
H_2	*Organisational Culture has a positive effect on Awareness of cybercrime within the public sector organisation.*	✔
H_3	*Cybercrime Awareness has a positive effect on the Ability to Report attacks from cybercrime within a public sector organisation.*	✔
H_4	*User Training on Information Security Awareness has a positive effect on Cybercrime Awareness.*	✔
H_5	*User Training on Information Security Awareness has a positive effect on Understanding of Information Security Regulations.*	✗
H_6	*User Training on Information Security Awareness has a positive effect on Ability to Report attacks from cybercrime within a public sector organisation.*	✔
H_7	*Understanding of Cybercrime Legislation has a positive effect on the Ability to Report attacks from cybercrime within a public sector organisation.*	✔

Table 18: Outlined Testing Results of Hypotheses

Comparison of how the R^2 values have changed between results of correlation analysis (Table 13) and multiple regression analysis are given below in Table 19.

Relationship	Construct	R value	R^2 Value	Multiple Regression R^2 Value
Reporting vs. Training	Training	0.42	0.18	0.32
Reporting vs. Awareness	Awareness	0.41	0.17	0.32
Reporting vs. Legislation	Legislation	0.29	0.08	0.32
Awareness vs. Culture	Culture	0.27	0.07	0.18
Awareness vs. Training	Training	0.35	0.12	0.18

Table 19: Comparison of R^2 values for Correlation and multiple regression results

From Table 19 it can be seen that the best improvement to R^2 values was on the Training construct (Reporting vs. Training), with a percentage increase from 0.18 to 0.32; followed by Awareness increasing from 0.17 to 0.32. For the Awareness dependent variable, the improvement on R^2 value also involved the Training construct from 0.12 to 0.18.

7.4 Hypothesis Testing and Discussion

In this section the results obtained for the hypotheses that were tested in the previous section will be discussed. This will be achieved by considering each hypothesis in relation to the literature from which it was suggested.

7.4.1 Hypothesis 1: Was Not Supported

$H_0$1: Organisational Culture has no effect on the ability to Report attacks from cybercrime within a public sector organisation.

$H_1$1: Organisational Culture has a positive effect on the ability to Report attacks from cybercrime within a public sector organisation.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_1	Organisational Culture (O_CULTURE)	Cybercrime Reporting (REPORTING)	0.961476	Accept null hypothesis ($H_0$1)

Table 20: Results Summary - Hypothesis 1

Table 20 above shows that the regression analysis for hypothesis H_1 produced a p-value of 0.96147 which is evidently greater than the threshold of 0.05. Therefore, this makes it impossible to reject the null hypothesis; hence this provides not enough evidence to prove that indeed organisation culture has an effect on the ability to report attacks from cybercrime in the public sector in Botswana. The implication from this is that even if public employees in Botswana may find that their organisational culture enabled them to perform better or be productive at work, they however did not think that it contributed to their ability to report cybercrime incidents that they experienced in their organisations.

The obtained results seem to be contradicting research by Malcolmson (2009) who reported that no matter how comprehensive the security policies for an organisation maybe, they are influenced by the culture of employees within that organisation. These results might however have been influenced by the considerably few responses that were obtained from the research.

7.4.2 Hypothesis 2: Was Supported

$H_0$2: Organisational Culture has no effect on Awareness of cybercrime within the public sector.

$H_1$2: Organisational Culture has a positive effect on Awareness of cybercrime within the public sector.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_2	Organisational Culture (O_CULTURE)	Cybercrime Awareness (AWARENESS)	0.035706	Reject null hypothesis ($H_0$2)

Table 21: Results Summary - Hypothesis 2

The above results shown in Table 21 supported this hypothesis (H_2) since it had a p-value of (0.035706) which was less than the 0.05 threshold. Therefore, this can be used as enough reason to reject the null hypothesis and furthermore provide ground for conclusion that there is evidence which is strong enough for inferring that Organisational Culture has a significant effect on Awareness of cybercrime within the public sector. Hence this means that the more enabling the organisational culture is for employees to be productive and efficient, then the more they will find it easier to be aware of cybercrime within the Botswana public sector. These results seem to be consistent with earlier research that was done by Malcolmson (2009) who noted that organisational culture has an impact in the successful enforcement of security on information systems in organisations; as a result management should formulate policies and practices that enable employees to be aware and adhere to information security measures. Furthermore, these results are still supported by other researchers (IAEA, 2008).

7.4.3 Hypothesis 3: Was Supported

$H_0$3: Cybercrime Awareness has no effect on the Ability to Report attacks from cybercrime within the public sector.

$H_1$3: Cybercrime Awareness has a positive effect on the Ability to Report attacks from cybercrime within the public sector.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_3	Cybercrime Awareness (AWARENESS)	Cybercrime Reporting (REPORTING)	0.015890	Reject null hypothesis ($H_0$3)

Table 22: Results Summary – Hypothesis 3

It is evident from Table 22 above that hypothesis H_3 fielded a p-value of (0.015890) which is far less than 0.05 and this gives enough evidence not to accept the null hypothesis; hence it can be inferred that indeed Cybercrime Awareness has a significant effect on the Ability to Report attacks from cybercrime within the public sector. The results obtained are endorsed by Arpana and Chauhan (2012) as well as Aloul (2010) who also showed that there is general

lack of cybercrime awareness by system users of different positions within organisations which contributes to less security breaches in the organisation being reported; hence if awareness was high then they will be more likely to report these incidents when they experience them.

7.4.4 Hypothesis 4: Was Supported

$H_0$4: User Training on Information Security Awareness has no effect on Cybercrime Awareness within the public sector.

$H_1$4: User Training on Information Security Awareness has a positive effect on Cybercrime Awareness within the public sector.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_4	User Training on Information Security Awareness (TRAINING)	Cybercrime Awareness (AWARENESS)	0.025918	Reject null hypothesis ($H_0$4)

Table 23: Results Summary - Hypothesis 4

The regression analysis for hypothesis H_4 (Table 23) obtained a p-value of 0.025918 which happens to be less than 0.05; this means the null hypothesis cannot be accepted. The conclusion for this is that enough evidence is available to warranty inferring that User Training on Information Security Awareness has a significant effect on Cybercrime Awareness. This means that if employees in the public sector have been provided training on information security awareness within their organisation, then they will be more aware of cybercrime incidents that they encounter. The above results are consistent findings by several researchers (Aloul, 2010; Cassim, 2009; Grobler & van Vuuren, 2010) who reported that information security training given to system users will equip them to be able to identify and respond to potential attacks against their system. This was also supported by Holmner et al., (2010) and Whitman and Mattord (2007).

7.4.5 Hypothesis 5: Not Supported

$H_0$5: User Training on Information Security Awareness has no effect on Understanding of Cybercrime Legislation.

$H_1$5: User Training on Information Security has a positive effect on Understanding of Cybercrime Legislation.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_5	User Training on Information Security Awareness (TRAINING)	Cybercrime Legislation (LEGISLATION)	0.076638	Accept null hypothesis ($H_0$5)

Table 24: Results Summary - Hypothesis 5

The results that were obtained from the regression analysis (Table 24) for hypothesis H_5 produced a p-value of 0.076638 which is greater than 0.05 which could not support this hypothesis. Therefore, this failed to provide sufficient evidence against the null hypothesis. Hence it can be inferred that User Training on Information Security Awareness has no effect on Understanding of Cybercrime Legislation. These findings are not in line with what has been reported by Aloul (2010) that to enable system users to have a better knowledge of the cybercrime legislation in their countries, these should be incorporated as components into existing information security training.

7.4.6 Hypothesis 6: Was Supported

$H_0$6: User Training on Information Security Awareness has no effect on Ability to Report attacks from cybercrime within the public sector.

$H_1$6: User Training has a positive effect on Ability to Report attacks from cybercrime within a public sector organisation.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_6	User Training on Information Security Awareness (TRAINING)	Cybercrime Reporting (REPORTING)	0.048580	Reject null hypothesis ($H_0$6)

Table 25: Results Summary - Hypothesis 6

It is evident from Table 25 above that hypothesis H_3 yielded a p-value of (0.048580) which is far less than 0.05 and this gives enough evidence not to accept the null hypothesis; hence it can be inferred that indeed User Training on Information Security Awareness has a significant effect on Ability to Report attacks from cybercrime within the public sector.

7.4.7 Hypothesis 7: Was Supported

$H_0$7: Understanding of Cybercrime Legislation has no effect on the Ability to Report attacks from cybercrime within the public sector.

$H_1$7: Understanding of Cybercrime Legislation has a positive effect on the Ability to Report attacks from cybercrime within the public sector.

Hypothesis	Independent Variable	Dependent Variable	p-level	Conclusion
H_7	Understanding of Cybercrime Legislation (LEGISLATION)	Cybercrime Reporting (REPORTING)	0.038603	Reject null hypothesis ($H_0$7)

Table 26: Results Summary - Hypothesis 7

The above results shown in Table 26 supported this hypothesis (H_2) since it had a p-value of (0.038603) which was less than the 0.05 threshold. Therefore, this can be used as enough reason to reject the null hypothesis and furthermore provide ground for conclusion that there is evidence which is strong enough for inferring that Understanding of Cybercrime Legislation has a significant effect on the Ability to Report attacks from cybercrime within the public sector. This is further supported by a number of authors (Cassim, 2009; Grobler & van Vuuren, 2010; Manda, 2011) who have highlighted the need for comprehensive cybercrime legislation that is needed to manage and control cybercrime.

7.5 Summary of Results and Refined Model

The four constructs listed below (from Section 3.4) were assumed to have an effect on the ability to report attacks from cybercrime in organisations within the public sector in Botswana. They are:

1. O_CULTURE: Organisational Culture.
2. AWARENESS: Cybercrime Awareness.
3. TRAINING: User Training on Information Security Awareness.
4. LEGISLATION: Understanding of Cybercrime Legislation.

The above constructs resulted in development of seven hypotheses which were then investigated through the data analysis stage. After analysing the data only five hypotheses were supported. Therefore, from the findings of the data analysis the initial research framework with hypotheses that was presented in Figure 8 was refined as shown in Figure 14 below; the coefficient values (r) for each relationship have also been shown with an asterisk (*) to indicate they are significant at $p<0.05$.

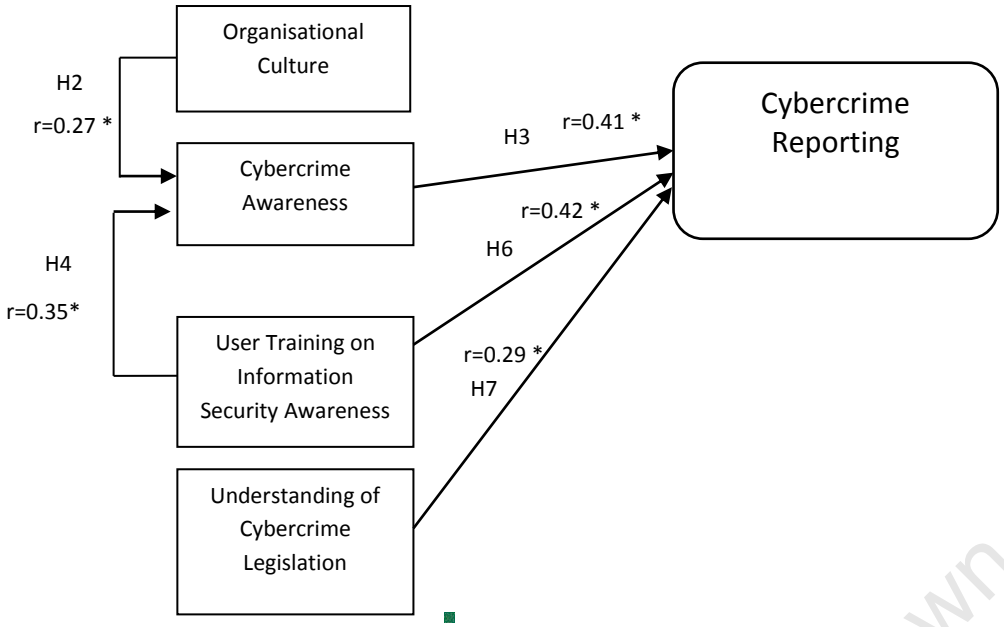

Figure 14: Refined Framework for Cybercrime Reporting

Chapter 8: Conclusions

8.1 Background

The government of Botswana has embraced the use of Information and Communication Technology (ICT) which is now wide spread in its different departments and public institutions around the country in order to improve productivity and efficiency for service delivery (Kyobe, 2010; Moloi & Mutula, 2007). This increase in ICT adoption has resulted in problems such as cybercrime to be realised even by the public sector in Botswana and other African countries due to poor controls and lack of cybercrime legislation that are needed to secure the infrastructure; hence criminals act as they please (Ngakaagae, 2010).

In response to the above situation this study was initiated with an aim to investigate factors that impact on the ability of the Botswana public sector from reporting properly on cybercrime attacks. Therefore, the study had the following main goal: developing a research framework and then validating it empirically within the Botswana public sector.

To develop this framework, previous academic literature on cybercrime and information security on the following areas was reviewed: cybercrime awareness (Aloul, 2010; Arpana & Chauhan, 2012; Malcolmson, 2009); user training on information security awareness (Cassim, 2009; Grobler & van Vuuren, 2010; Holmner et al., 2010); organisational culture (Malcolmson, 2009; Uttal, 1983); and cybercrime legislation (Cassim, 2009; Grobler & van Vuuren, 2010; Manda, 2011). These were used to build the framework for Cybercrime Reporting. In the assessed literature available on cybercrime, no suitable research framework was identified which could be used to address the area that was under investigation. Therefore, concepts that were gathered from literature were synthesised to develop a framework that was later tested in the study.

8.2 Testing of Research Framework

The research instrument was tested for quality and validity through piloting. Furthermore, data obtained from the questionnaires was statistically tested against the hypotheses that were developed for the research framework constructs. The research instrument was also checked for reliability and validity, and finally correlation and multiple linear regressions analysis were carried out to test the hypotheses.

8.3 Key Findings

The results from this study helped to reveal which independent variables of the research framework (AWARENESS, O_CULTURE, LEGISLATION, and TRAINING) had an impact on the dependent variable (REPORTING). It emerged that Cybercrime Awareness (AWARENESS), Understanding of Cybercrime Legislation (LEGISLATION) and User Training on Information Security Awareness (TRAINING) were the only ones that significantly affected Cybercrime Reporting (REPORTING); while Organisational Culture (O_CULTURE) did not. On the other hand, Cybercrime Awareness (AWARENESS) was found to be significantly affected by Organisational Culture (O_CULTURE) and User Training on Information Security Awareness (TRAINING). Most of these results were consistent with what other studies that were used to develop the research framework had reported.

The result from the analysis of the 5 constructs together with the 5 hypotheses relationships that were supported in the multiple regression analysis provide a sufficient way to understand the interaction between Organisational Culture, Cybercrime Awareness, User Training on Information Security Awareness, Understanding of Cybercrime Legislation, and Cybercrime Reporting in the Botswana public sector.

8.4 Implications for Academics

Several studies have addressed the growing problem of cybercrime in Africa and globally due to an increase in ICT and also lately due to increase in broadband access. Most of these studies have been conducted in the developed countries; hence they may not provide meaningful solutions for many of the developing countries that have different contexts or situations from those that are present in developed nations. Furthermore, these studies have addressed cybercrime mostly from the private sector perspective which is mainly profit driven and hence has more incentives to address the problem. Fewer studies have addressed cybercrime in the government or public sector given the increase in ICT use.

Therefore, this research will contribute to the body of knowledge in IS/IT literature on cybercrime, with emphases on provision of a solution (framework) to help address this growing problem. The framework produced by this study was adequately validated and

shown to be reliable for use, and can be used in future quantitative studies to determine factors that affect the ability for reporting of cybercrime for organisations in other non-profit making sectors. Furthermore, the inclusion of organisational culture in this framework is a significant contribution to the research field of IS towards the management of cybercrime since it emphasises the interaction of human beings and ICT. Other IS researchers can expand and modify this framework in order to apply in other sectors and countries.

8.5 Implications for Practitioners

Results obtained from this study can significantly be of benefit to the Botswana Government in its efforts to address the issue of cybercrime reporting among its employees. First of all, the Botswana Government can adopt the developed research framework in all its ministries (organisations) in order to ensure that there is a unified way of dealing with cybercrime. This will enable ministries that had already put in place measures to tackle this problem to be able to realign their efforts accordingly, while providing the ones that had not yet started to address it with a guideline to follow.

Adopting findings from this study can be done in such a way that they are integrated into already existing programmes within the organisations, such as training on ICT use for employees, and general induction training for new employees. Contents of these training programmes could incorporate Cybercrime Awareness, Information Security matters and concepts of the Cybercrime Legislation of Botswana for instance, so that the employees are made aware of this problem at the initial time that they start using ICTs. This would help them to appreciate the risks that are involved with using ICT as far as cybercrime is concerned. Hopefully this knowledge will make users more vigilant and also report most incidents that they encounter.

Results of this study can also help top management in government organisations to appreciate and understand that the problem of cybercrime is not only the responsibility of the IT department alone, but rather involves everyone in the organisation. Therefore, this could help to motivate management to include cybercrime management in their strategies and also allocate sufficient resources needed to address it.

Another important finding of this study is that Cybercrime Reporting is dependent on a number of factors (constructs), which should be put in place to enable users to report easily. Therefore, this implies that an environment conducive for reporting should be created. Part of this involves having a facility where incidents can be reported, and also training the IT officers to be able to understand how to handle cybercrime incidents that are reported to them. Therefore, this would require that incidents should be managed properly, and furthermore the IT environment should also be conducive to collect evidence (digital forensic readiness) relating to these incidents when the need arises (Saint-Germain, 2005).

8.6 Limitations and Further Research

There are a number of limitations that have be considered while interpreting results from this study, these can also form bases for future research in order to expand its scope. The limitations include the sample for the study and also the procedure that was used to collect the data.

The study sample was focused on views of top management, human resources (HR) department, IT department, and general IT users within different government organisations (ministries) in the capital city (Gaborone). However this sample left out many other departments and areas of Botswana which might be using ICT more than the selected sample. Furthermore, the number of respondents that was obtained from this study was small compared to the total number of employees in Botswana public sector.

Furthermore, the study did not use any demographics such as department, age or gender as independent variables. This was only summarised with descriptive statistics and representations through graphs. Therefore, further studies could conduct some statistical analysis to determine the effects of demographic profiles on cybercrime awareness and reporting.

The last limitation was that this was a cross sectional study; therefore, future studies could use a longitudinal time frame to examine how reporting changed over time.

8.7 Conclusion

This research proposed a framework which presents the essential features that are needed for users of ICT in public organisations in Botswana to be able to report cybercrime incidents or attacks that they experience. This was achieved after collecting data and empirically analysing it; thereby three elements (Cybercrime Awareness, User Training on Information Security Awareness, and Understanding of Cybercrime Legislation) were found to have statistically significant impact on the ability of users' Reporting of Cybercrime incidents that they experienced. Furthermore, Organisational Culture and User Training on Information Security Awareness were also found to be statistically significantly impacting on Cybercrime Awareness in the Botswana public sector.

This study expands on the body of knowledge that is currently available on the impact of an increase in ICT investment by governments especially in Africa and other developing nations, which results in problems such as cybercrime; hence the study contributes by suggesting a solution to deal with this problem. Finally, it is anticipated that results of this study will motivate other scholars to expand on the issue of cybercrime reporting in other sectors and countries that have invested on ICT to enhance their operations and improve efficiency. These research findings can also be implemented by the Botswana Government to address the problem of cybercrime that is being experienced.

Chapter 9: References

Akuta, E. A. M., Ong'oa, I. M., Jones, C. R. (2011). Combating cyber crime in Sub-Sahara Africa: A discourse on law, policy and practice. *Journal of Peace, Gender and Development Studies*, 1(4), 129-137.

Ali, S., & Green, P. (2007). IT governance mechanisms in public sector organisations: an Australian context. *Journal of Information Management*, 15(4), 41-63.

Aloul, F. A. (2010). *Information security awareness in UAE: A survey paper*. Internet Technology and Secured Transactions (ICITST) 2010 International Conference, November 8-11, 2010. Retrieved December 7, 2011, from IEEE Xplore Digital Library.

Altman, I. (1975). *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding.* Monterey, CA: Brooks/Cole Pub. Co., Inc.

Anderson, R., & More, T. (2006). The economics of information security. *Science Magazine*. 314(5799), 610 – 613. Retrieved April 4, 2011, from http://www.sciencemag.org/cgi/content/full/sci;314/5799/610

APWG. (2009). *Phishing activity trends report: Q4 2009*. Retrieved May 20, 2011 from http://www.antiphishing.org/reportslapwg_ report_Q4 2009.pdf.

APWG. (2011). *Global phishing survey: Trends and domain names use in 2010*. Retrieved June 16, 2011, from http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf .

Archick, K. (2004). *Cybercrime: Council of Europe Convention: CSC report for congress*. Retrieved April 24, 2011, from http://fpc.state.gov/documents/organization/36076.pdf

Arpana, M., & Chauhan, M. (2012). Preventing cyber crime: A study regarding awareness of cyber crime in Tricity. *International Journal of Enterprise Computing and Business Systems, 2*(1), 1-10.

Association for Information Systems. (2010). *Qualitative, positivist research in information systems*. Retrieved December 16, 2011, from http://ais.affiniscape.com/displaycommon.cfm?an=1&subarticlenbr=495

Barske, D., Stander, A. & Jordaan, J. (2010). *A digital forensic readiness framework for South Africa*. In Information Security for South Africa Conference, Santon, Johannesburg, August 2-4, 2010. Retrieved September 14, 2011, from IEEE Xplore Digital Library.

Becker, H. S., & Geer, B. (1970). *Participant observation and interviewing: A comparison*. In W. Filstead (Ed.), Qualitative methodology. Chicago: Rand McNally, 133-142.

Bennett, M. (2006, April 6). British FBI drops confidentiality charter for it crime victims. *IT Week.* Retrieved from April 23, 2012, from http://www.computing.co.uk/ctg/news/1830868/british-fbi-drops-confidentiality-charter-it-crime-victims

Berlyne, D. (1965). *Structure and direction in thinking*. New York: John Wiley and Sons Inc.

BERR. (2008) *Information breaches security survey 2008: Technical report.* London: Department of Trade and Industry.

Blakley, B., McDermott, E, & Geer, D. (2001).*Information security is information risk management*. In Proceedings of the 2001 workshop on New security paradigms. New York, NY, USA. Retrieved November 15, 2011, from ACM Digital Library.

Bluedorn, A. C., & Lundgren, E. F. (1993). A culture-match perspective for strategic change, *Research In Organizational Change and Development*, 7, 137–179.

Bonebright, T. L., Miner, N. E., Goldsmith, T. E., & Caudell, T. P. (2005). Data collection and analysis techniques for evaluating the perceptual qualities of auditory stimuli. *ACM Transactions on Applied Perceptions, 2*(4), 505-516.

Botswana Gazette. (2008, June 3). *CMS P17m fraud case starts*. Retrieved April 13, 2011, from http://www.gazettebw.com/index.php?option=com_content&view=article&id=913:cms-p17m-fraud-case-starts&catid=18:headlines&Itemid=1

Brenner, S. W. (2004). Cybercrime metrics: Old wine, new bottles? *Virginia Journal of Law & Technology*, 9(4), 1-52.

Brown, I. T. J., & Jayakody, R. (2008). B2C e-commerce success: A test and validation of a revised conceptual model. *Electronic Journal of IS Evaluation*, 11(3), 167-184.

Burnes, B., Cooper, C., & West, P. (2003). Organisational learning: The new management paradigm? *Management Decision*, 41(5), 452-64.

Businessweek. (2012). *Cyber crime and information warfare: A 30 year history*. Retrieved November 13, 2012, from http://images.businessweek.com/ss/10/10/1014_cyber_attacks/index.htm

Bwalya, K. J. (2010). E-government implementation in Botswana: A snapshot view. *Information Technology in Developing Countries.* Retrieved November 19, 2011, from http://www.iimahd.ernet.in/egov/ifip/kelvin.htm

Cambini, C., & Jiang, Y. (2009). Broadband investment and regulation: A literature review. *Telecommunications Policy*, 33, 559-574.

Cameron, R. D., & Stone, A. B. (1995). *Serving the public service*. Pretoria: Van. Schail

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, Journal *of Computer Security*, 11(3), 431-448.

Canhoto, A. (2010). *'What' before 'How'*. Oxford Internet Institute Forum. Retrieved May 10, 2011, from http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf

Cardoso, L. S. (2007). Cyber crime and critical information infrastructure impact. *International Telecommunication Union*. Retrieved April 12, 2011, from http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/cardoso-cybercrime-impact-praia-nov-07.pdf

Casey, E. (2004). *Digital Evidence and Computer Crime* (2nd ed.). London: Academic Press

Casey, E. (2006). Investigating sophisticated security breaches. *Communications of the ACM*, 49(2), 48-54.

Cassim, F. (2009). Formulating specialised legislation to address the growing spectre of cybercrime: A comperative study. *PER*, 12(4), 36-79.

Cavana, R. Y., Delahaye, B. R., & Sekaran, U. (2001). *Applied business research: Qualitative and quantitative methods* (3rd ed.). Australia: John Wiley.

Chiesa, R. (2010). *Cybercrime reasons evolution of the players and an analysis of their modus operandi*. Retrieved May 14, 2011, from http://www.flarenetwork.org/report/enquiries/article/cybercrime_reasons_evolution_of_the_players_and_an_analysis_of_their_modus_operandi.htm

Coates, J., F. (2002). What's next? Foreseeable terrorist acts. *The Futurist*, 36(5), 23-36.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., & Goodman, S. E. (2008). *Cybersecurity in Africa: An assessment*. Atlanta, Georgia: Sam Nunn School of International Affairs, Georgia Institute of Technology.

Computer Security Institute. (2011). *15th Annual 2010/2011 computer crime and security survey*. Retrieved May 17, 2012, from https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

Conference of State Bank Supervisors. (2010). *Executive Summary of the Sarbenes-Oxley Act of 2002 P.L.107-204*. Retrieved July 10, 2011, from http://www.csbs.org/legislative/leg-updates/Documents/ExecSummary-SarbanesOxley-2002.pdf

Cottrell, R. L., & Kalim, U. (2009). *New E. coast of Africa fibre*. Retrieved January 20, 2012, from https://confluence.slac.stanford.edu/display/IEPM/New+E.+Coast+of+Africa+Fibre

Council of Europe. (2012). *The Council of Europe in brief: Who we are*. Retrieved December 17, 2011, from http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=en

Danielsson, J., & Tjostheim, I. (2004). *The need for a structured approach to digital forensic readiness.* IADIS International Conference E-commerce, Lisbon. Retrieved November 15, 2011, from http://www.iadis.net/dl/final_uploads/200406C018.pdf

Deal, T. E., & Kennedy, A. A. (1982). *Corporate Cultures*. Reading, MA: Addison-Wesley.

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behaviour*. New York: Plenum Press.

DeCoster, J. (1998). *Overview of factor analysis*. Retrieved January 17, 2012, from http://www.stat-help.com/notes.html

Deloitte. (2011). *Public governance and accountability*. Retrieved July 2, 2011, from http://www.deloitte.com/view/en_GX/global/industries/public-sector/public-governance-and-accountability/index.htm

Department of Energy. (2009). *Cyber security incident management manual*. Retrieved May 12, 2011 from https://www.directives.doe.gov/directives/current-directives/205.1-DManual-8/at_download/file

Department of Treasury and Finance. (2007). *Victorian government risk management framework.* Retrieved May 10, 2011, from

http://www.vmia.vic.gov.au/~/media/Content-Documents/Risk-Management/Guides-and-Publications/Risk-Management-Guidelines/government-risk-managment-framework.ashx

Downe-Wamboldt, B. (1992). Content analysis: Method, applications, and issues. *Health Care for Women International*, 13, 313-321.

El Kettani, M. D. E., & Debbagh, T. (2008). *NCSec: A national cyber security referential for the development of a code of practice in national cyber security management*. In Proceedings of the 2nd international conference on Theory and practice of electronic governance. New York, NY, USA. Retrieved November 15, 2011, from ACM Digital Library.

Fafinski, S. (2007). *UK cybercrime report*. Retrieved May 14, 2011, from https://www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf

Fafinski, S., Dutton, W. H., & Margetts, H. (2010). *Mapping and measuring cybercrime*. OII Forum Discussion Paper No. 18. Oxford Internet Institute: University of Oxford. Retrieved from April 9, 2012, from http://www.oii.ox.ac.uk/publications/FD18.pdf

Ferwerd, J., Choucri, N., & Madnick, S. (2010). *Institutional foundations for cyber security: Current responses and new challenges*. Retrieved November 13, 2012, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA530584

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Marketing Research Journal, 18*(1), 39-50.

Garson, G. D. (2008). *Multiple regression*. Retrieved May 5, 2012, from http://faculty.chass.ncsu.edu/garson/PA765/regress.htm

Ghauri, P., & Gronhaug, K. (2002). *Research methods in business studies*: *A practical guide*. United Kingdom: Prentice Hall.

Gordon, S., & Ford, R. (2006). On the definition and classification of cyber crime. *Journal in Computer Virology*, 2(1), 13-20.

Grobler, M. & van Vuuren, J., J. 2010. *Broadband broadens scope for cyber crime in Africa*. *Proceedings of the 2010 Information Security for South Africa conference*. Sandton, South Africa, 2 - 4 August 2010, pp 1-8.

Guerra, P. (2009). *How economics and information security affects cybercrime and what this means in the context of a global recession*. Retrieved April 11, 2011, from http://www.blackhat.com/presentations/bh-usa-09/GUERRA/BHUSA09-Guerra-EconomicsCyberCrime-SLIDES.pdf.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis*. New Jersey: Pearson Prentice Hall.

Hair, J., F., Anderson, R., E., Tatham, R., L., & Black, W., C. (1998). *Multivariate Data Analysis, (5th ed)*. Upper Saddle River, NJ: Prentice Hall.

Harrington , S., & Niehau, G. (1999). *Risk Management and Insurance*. Boston, Irwin: McGraw Hill.

Hart, M. L., Esat, F., Rocha, M., & Khatieb, Z. (2007). Introducing students to business intelligence: Acceptance and perceptions of OLAP Software. *Journal of Issues in Informing Science and Information Technology*, *4*, 105-123.

Hirschauer, N., & Musshoff, O. (2007). A game-theoretic approach to behavioral food risks: The case of grain producers. *Food Policy*, 32(2), 246-265.

Hirshleifer, J. (1998). The bioeconomic causes of war. *Managerial and Decision Economics*, 19(7/8),457-466.

Hofstede, G. (2007) *Geert Hofstede cultural dimensions*. Retrieved May 12, 2011, from http://www.geert-hofstede.com/

Hofstede, G., & Hofstede, G. J. (2004) *Cultures and Organizations: Software of the Mind*. New York: McGraw-Hill.

Holmner, M., Britz, J. J., & Ponelis, S. R. (2010). The last mile or the lost mile? The information and knowledge society in Africa. *Proceedings of SIG GlobDev Third Annual Workshop*, Saint Louis, USA.

Husted, B. W. (2000). The impact of national culture on software piracy. *Journal of Business Ethics*, 26(3), 197-211.

IAEA. (2008). *Nuclear security culture: implementing guide*. Vienna: International Atomic Energy Agency.

Imtiaz, F. (2006*). Enterprise computer forensics: A defensive and offensive strategy to fight computer crime*. Proceedings of the 4th Australian Digital Forensic Conference, Edith-Cowan University, Perth, December 4, 2006.

Internet World Stats. (2011). *Usage and population statistics: Africa*. Retrieved February 18, 2012, from http://www.internetworldstats.com/africa.htm#bw

IST-Africa. (2012). *Introduction: Republic of Botswana*. Retrieved January 20, 2012, from http://www.ist-africa.org/home/default.asp?page=doc-by-id&docid=5195

ITU. (2009). *Understanding cybercrime: A guide for developing countries*. International Telecommunication Union (ITU). Retrieved September 10, 2011, from http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFE.pdf

Kirk, J. (2009, March 11). Countries move forward on cybercrime treaty. *PC World*. Retrieved December 11, 2011, from http://www.pcworld.com/article/161067/countries_move_forward_on_cybercrime_treaty.html

KPMG. (2009). *Corporate governance and king 3, advisory*. Retrieved July 12, 2011, from http://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Tax-and-Legal-Publications/Documents/Corporate%20Governance%20and%20King%203.pdf

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11, 541-562.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security and Privacy*, 4(1), 33-39.

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Heidelberg: Springer.

Kyobe, M. (2010). *Information Security challenges and their implications for emerging e-government structures in some African Countries*. 4th IDIA Conference, pp. 1-13.

Leedy, P. & Ormrod, J. (2005). *A handbook for teacher research from design to implementation*. New Jersey: Pearson Education.

Lipchak, A. and McDonald, J. (2003).*E-government and e-records readiness and capacity building, discussion paper*. Retrieved May 22, 2011, from http://irmt.org/download/DOCUME%E2%88%BC1/GLOBAL/discussionpaper.pdf

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal use of information & communication technologies in Sub-Sahara Africa: Trends, concerns and perspectives. *Journal of Information Technology Impact*, 9(3), 155-172.

Lucas, H. C. (1991). Methodological issues in information survey research. In K. L. Kraemer (Ed.), *The Information Systems Research Challenge: Survey Research Methods*, pp. 273-285. Boston, MA: Harvard Business School.

Madiya, P. (2012, April 13). New interpol rules compromise fight against cyber crime. *Mmegi* . Retrieved April 14, 2012, from http://mmegi.bw/index.php?sid=1&aid=224&dir=2012/April/Friday13

Malcolmson, J. (2009). *What is security culture? Does it differ in content from general organisational culture?* Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference, pp.361-366, 5-8 Oct. 2009 Retrieved November 14, 2011, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5335511&tag=1

Manda, T. D. (2011). *Maturity of cybersecurity initiatives in Malawi: A comparison with the drive for fast and ubiquitous Internet connectivity*. Retrieved May 10, 2012, from http://www.v01.diplomacy.edu/sites/default/files/IGCBP2010_2011_Manda.pdf

Mandia, K., & Prosise, C. (2001). *Incident Response*. Berkley: Osborne McGraw-Hill.

Marion, N. E. (2010). The Council of Europe's cyber crime treaty: An exercise in symbolic legislation. *International Journal of Cyber Criminology*, 4(1&2), 699-712.

Martin, J., & Siehi, C. (1983). Organisational culture and counterculture: An uneasy symbiosis. *Organisational Dynamics*, 12(2), 52-64.

Merenda, P. F. (1997). A guide to the proper use of factor analysis in the conduct and reporting of research: Pitfalls to Avoid. *Measurement and Evaluation in Counseling and Development*, 30, 156-164.

Mmegi. (2011, March 7). *Court finds 5 guilty in CMS fraud case*. Retrieved April 21, 2011, from http://www.mmegi.bw/index.php?sid=1aid=2387dir=2010/May/Friday14&aid=1513&dir=2011/March/Monday7

Mmegi. (2012, June 13). *Questionable absence of DPSM at the ILO convention in Geneva*. Retrieved June 15, 2012, from http://mmegi.bw/index.php?sid=10&aid=866&dir=2012/June/Wednesday13

Molla, A., & Licker, P. S. (2001). E-commerce systems success: An attempt to extend and respecify the Delone and McLean Model of IS Success. *Journal of Electronic Commerce Research, 2*(4), 131-141.

Moloi, J., & Mutula, S. (2007). E-record management in an e-government setting in Botswana. *Sage*, 23(4), 290-306.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, 27(3), 27-32.

Morawczynski, O., & Ngwenyama, O. (2007). Unravelling the impact of investment in ICT, education and health on development: An analysis of archival data of five West African countries using regression splines. *The Electronic Journal on Information Systems in Developing Countries*, 29(5), 1-15.

Mutua, W. (2011, July 5). The state of e-governance/e-government in Africa. *African innovation*, Retrieved February 19, 2012, from http://afrinnovator.com/blog/2011/07/05/the-state-of-e-governancee-government-in-africa

Mutula, S., M. (2002). Current developments in the Internet industry in Botswana. *The Electronic Library*, 20(6), 504-511.

Nagpal, R. (2008). *Evolution of cyber crimes*. Retrieved May 11, 2011, from http://www.asianlaws.org/library/cci/evolution-cyber-crime.pdf

Natsui, T. (2003). *Cybercrime in Japan: Recent cases, legislation, problems and perspectives*. Retrieved November 20, 2011, from http://www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf

Nunnally, J. (1978). *Psychometric theory*. New York: McGraw-Hill.

Nyanda, S. (2010). *Notice of intention to make South African national security cybersecurity policy*. Government Gazette (Vol. 536, No 32963). Pretoria Retrieved December 14, 2011, from http://www.pmg.org.za/files/docs/100219cybersecurity.pdf

O'Reilly, C. A., & Chatman, J. A. (1996). Culture as social control: Corporations, cults, and commitment. *Research in Organisational Behaviour*, 18,175-200.

Ochieng, Z. (2011, May 2). Africa: Cybercrime on the rise as bandwidth increases. *News From Africa*. Retrieved August 2, 2011, from http://www.newsfromafrica.org/newsfromafrica/articles/art_12536.html

OECD. (2005). *Spam issues in developing countries*. Paris: Organisation for Economic Cooperation and Development (OECD).

OECD. (2008). *African economic outlook: Botswana*. Retrieved February 15, 2012, from http://www.oecd.org/dataoecd/14/36/40573959.pdf

Palen, L. & Dourish, P. (2003). *Unpacking privacy for a networked world*. In Proceedings of the SIGCHI conference on Human factors in computing. New York, NY, USA. Retrieved May 20, 2011, from ACM Digital Library.

Parson, N. (1999). *A New History of Botswana*. Gaborone: Macmillan.

Peterson, R. A. (2000). A meta-analysis of variance accounted for and factor loadings in exploratory factor analysis. *Marketing Letters*, 11 (3), 261-267.

Pettigrew, A. M. (1979). On studying organizational cultures. *Administrative Science Quarterly*, 24, 570-581.

Pindyck, R., & Rubinfeld, D. (1998). *Econometrics model and economic forecasts*. Singapore: McGraw-Hill.

Price Water House Coopers. (2009). *King's counsel: Understanding and unlocking the benefits of sound corporate governance*. Retrieved July 10, 2011, from http://www.pwc.com/za/en/assets/pdf/Executive-Guide-to-KINGIII-public-sector-guide-02.pdf

Public Administration Programme. (2010, January 1). United Nations e-government

development database. *United Nations Online Network in Public Administration and Finance - UNPAN*. Retrieved February 19, 2012, from http://www2.unpan.org/egovkb/datacenter/CountryView.aspx

Rashid, Z. A., Sambasivan, M., & Johari, J. (2003). The influence of corporate culture and organisational commitment on performance. *Journal of Management Development*, 22(8), 708-728.

Republic of Botswana. (2007). *Cybercrime and computer related crimes: Act NO.22 of 2007*. Gaborone: Government Printer.

Republic of Botswana. (2010). *1 gov: Botswana national e-government strategy 2011-2016*. Gaborone: Office of the President.

Rho, J. J. (2007). Blackbeards of the twenty-first century: Holding cybercriminals liable under the Alien tort statute. *Chicago Journal of International Law*, 7(2), 695-719.

Richardson, R. (2007). *The CSI computer crime and security survey.* Retrieved from April 10, 2012, from http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

Roscoe, J. T. (1975). *Fundamental research statistics for the behavioural sciences*. New York: Holt Rinehart & Winston.

Rosenau, J. N. (1995). Security in a turbulent world. *Current History*, *94*(592), 193-200.

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3), 1-28.

Rustad, M. L. (2001). Private enforcement of cybercrime on electronic frontier. *Southern Californian Law Journal*, 11, 63-116.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *The Information Management Journal*, 39(4), 60-66.

Schein, E. (1999). *The corporate culture survival guide*. San Francisco: Bass Jossey.

Schein, E.,H. (1985). *Organisational culture and leadership*. San Francisco, CA: Jossey-Bass.

Schwarz, (2007). *Legal foundation and development: The risk of cybercrime and its impact on Africa*. Retrieved May 14, 2011, from http://www.itu.int/ITU-D/cyb/events/2007/praia/docs/schwartz-legal-development-praia-nov-07.pdf

Shackelford, S. J. (2009). From nuclear war to net war: Analogizing cyber attacks in international law, *Berkeley Journal of International Law*, 27(1), 192-251.

Silicon Republic. (2009). *Cybercriminals make US$11,00 a day through SEO errors.* Retrieved May 5, 2011, from http://www.siliconrepublic.com/strategy/item/12555-cybercriminals-make-us-11-0

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *The Journal of Research in Crime and Delinquency*, 34, 495–518.

Smith, A. D. (2004). Cyberciminal impacts on online business and consumer confidence. *Online Information Review*, 28 (3), 224-234.

Sommer, P. (2009). *Directors and Corporate Advisors Guide to Digital Investigations and Evidence* (2nd ed). London: Information Assurance Advisory Council.

Sosa, G. C. (n.d). *Country report on cybercrime: The Philippines*. Retrieved May 13, 2011, from http://www.unafei.or.jp/english/pdf/RS_No79/No79_12PA_Sosa.pdf

Soxlaw. (2006). *A guide to the Sarbanes-Oxley Act*. Retrieved July 9, 2011, from http://www.soxlaw.com/index.htm

Sukhai, N. B. (2004). *Hacking and cybercrime*. Proceedings of the 1st annual conference on Information security curriculum development. New York, NY, USA. Retrieved January 24, 2011 from ACM Digital Library.

Symantec Corporation. (2012). *Internet security threat report: 2011 trends*. Retrieved May 27, 2012, from http://www.cert-hungary.hu/sites/default/files/news/symantec_internetbiztonsag_tanulmany_eng.pdf

Swardson, A. (2000, May 17). Multi-nation conference confronts cybercrime: Officials warn virus attacks are virtually unpreventable. *The Washington Post*. Retrieved November 24, 2011 from the High Beam Research database.

Tan, M., & Teo, T. (2000). Factors influencing the adoption of Internet banking. *Journal of the Association for Information Systems, 1*(5), 1-42.

Think Quest. (2011). *History of hacking*. Retrieved May 11, 2011, from http://library.thinkquest.org/04oct/00460/phishingHistory.html

Thomson, K., Von Solms, R., & Louw, L. (2006).Cultivating an organisational information security culture. *Computers Fraud & Security*, 10, 7-11.

United Nations. (1995). *The United Nations manual on the prevention and control of computer related crime*, 1995, supra note 41, paragraphs 20 to 73 in International Review of Criminal Policy, pp. 43–44.

United Nations. (2007). *Public governance indicators: A literature review*. New York: Department of Economic and Social Affairs. Retrieved July 11, 2011, from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan027075.pdf

United Nations. (2010). *United Nations e-government development database*. Retrieved December 19, 2011, from http://unpan3.un.org/egovkb/datacenter/countryview.aspx

US-CERT. (2012). *About us*. Retrieved November 13, 2012, from http://www.us-cert.gov/about-us/

Uttal, B. (1983). The corporate culture vultures. *Fortune*, 108(8), 66-72.

Vacca, J. R. (2005). *Computer Forensics: Computer Crime Scene Investigation*. (2nd ed). Boston: Charles River Media.

Valeri, L., Somers, G., Robinson, N., Graux, H., & Dumortier, J. (2006). *Handbook of Legal Procedures of Computer and Network Misuse in European Countries: Technical Report*. Brussels: Rand Europe.

Van der Heijden, H. (2003). Factors influencing the usage of websites: The case of a generic portal in The Netherlands. *Information and Management*, *40*(6), 541-549.

Van Niekerk, J. F., & Von Solms, R. (2009). Information security culture: A management perspective. *Computers & Security*, 29, 476-486.

Veerasamy, N., & Taute, B. (2009). *Introduction to emerging threats and vulnerabilities to create user awareness*, Information Security South Africa (ISSA2009) Conference, University of Johannesburg, Gauteng, South Africa, 6 - 8 July, 2009. Retrieved November 15, 2011, from http://researchspace.csir.co.za/dspace/handle/10204/3534

Volk, N. (2010). *Threat based risk management in the federal sector.* In 2010 Information Security Curriculum Development Conference, New York, NY, USA. Retrieved March 15, 2011 from ACM Digital Library.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23, 191-198.

Wall, D. S. (2007). *Cybercrime: The Transformation of Technology in the Networked Age*. Cambridge: Polity Press.

Webber, R. P. (1990). *Basic content analysis*. Beverly Hills, CA: Sage.

West-Brown, M. J., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for Computer Security Incident Response Teams* (2nd ed). Pittsburg: Carnegie Mellon Software Engineering Institute.

Whitman, M., & Mattord, H. (2007). *Principles of Information Security* (2 ed.). Boston: Course Technology.

Wilson, D., Patterson, A., Powell, G., & Hembury, R. (2006). *Fraud and technology crimes. findings from the 2003/04 British crime survey, the 2004 offending, crime and justice survey and administrative sources.* London: Home Office.

Zatyko, K. (2007). Defining digital forensics. *Forensic Magazine,* 4 (1), 18-22.

Appendix A: Cover Letter

Department of Information Systems
Leslie Commerce Building
Engineering Mall. Upper Campus
OR Private Bag. Rondebosch 77001
Cape Town
Tel: 650-2261
Fax No: (021) 650-2280

Dear Sir / Madam

Questionnaire on Cybercrime Awareness and Reporting in the Public Sector in Botswana

I am an Information Systems Masters student at the University of Cape Town (UCT) conducting research on factors that inhibit cybercrime awareness and reporting in the Botswana public sector. The attached questionnaire is aimed at the IT, Human Resources or Administration departments, Senior Management and General Computer Users. Factors that contribute to poor cybercrime awareness and reporting have been identified and presented in the questionnaire.

This questionnaire focuses on organisational culture, human behaviour, incident management, user training on information security awareness and lastly understanding information security regulations within your organisation. The main aim is to gain an understanding into how your organisation deals with these issues.

You are kindly requested to participate in this research by completing the attached questionnaire. The results of this study can be made available to participants on request. The information that is collected during this research shall be used for purposes of this research only and the responses shall be kept strictly confidential.

Yours faithfully

Sinka Matengu
(Masters Student)
sinka.matengu@uct.ac.za

Adrie.Stander
(Supervisor)
Office number: +27 21 650 4254
adrie.stander@uct.ac.za

Appendix B: Research Permit

Telephone: (267) 363200
FAX (267) 353100
TELEGRAMS: RABONGAKA
TELEX: 2818 CARE BD

MINISTRY OF HEALTH
PRIVATE BAG 0038
GABORONE

REPUBLIC OF BOTSWANA

REF NO: PPME-13/18/1 Vol VII (98) 13 September 2011

Sinka Matengu
P.O. Box 3
Kasane

Dear Mr Matengu

EXEMPTION: CYBERCRIME AWARENESS AND REPORTING IN THE PUBLIC SECTOR IN BOTSWANA

Reference is made to your application dated 12 September 2011 submitted to the Health Research Unit (HRU) for permission to conduct Cybercrime Awareness and Reporting in the Public Sector in Botswana. The HRU granted permission as the study poses no more than minimal risk and is therefore categorized as exempt research.

Permission is therefore granted to conduct the above mentioned study.. This approval is valid for a period of 1 year effective 13 September 2011.

This permit does not however grant you authority to collect data from the selected organizations without prior approval from their management. Consent from identifiable individuals should be obtained.

Furthermore, you are requested to submit a copy of the report or publication from this activity to the Health Research Division as part of dissemination of findings for our data base and library.

Yours sincerely

P. Khulumani
For Permanent Secretary

MINISTRY OF HEALTH
DEPT. OF POLICY PLANNING, MONITORING AND EVALUATION
13 SEP 2011
PRIVATE BAG 0038
GABORONE
REPUBLIC OF BOTSWANA

1

Appendix C: Questionnaire

Research Questionnaire: **Cybercrime Awareness and Reporting in the Public Sector in Botswana**

Instructions: *Please answer the following questions in relation to your organisation regarding cybercrime or computer attacks, by selecting the most relevant option.*

Demographics								
Ministry Name:	**Department:**	**Gender: (tick)**		**Age: (tick age group)**				
		Male	Female	21-34	35-44	45-54	55-64	65+
Nationality:								

Awareness						
	In this section, please rate the following statements:	**Not at all 1**	**Little 2**	**Average 3**	**More than Average 4**	**A lot 5**
1	I understand what cybercrime is	1	2	3	4	5
2	I can identify cybercrime incidents/attacks	1	2	3	4	5
3	I know how to protect myself from cybercrime	1	2	3	4	5
4	I understand the impact of cybercrime to my organisation	1	2	3	4	5
Cybercrime Legislation						
	Please rate the following statements:	**Not at all 1**	**Little 2**	**Average 3**	**More than Average 4**	**A lot 5**
5	I know about the cybercrime law of Botswana (Cybercrime & Computer Related Crimes Act)	1	2	3	4	5
6	I know the contents of the cybercrime law of Botswana	1	2	3	4	5
7	My organisation makes its employees aware of the cybercrime law	1	2	3	4	5
8	I know that the cybercrime law is helpful to address cybercrime in my organisation	1	2	3	4	5
Organisational Culture						
9	My organisation makes it easy for the staff members to report any issues of concern	1	2	3	4	5
10	My organisation mostly informs all employees about critical or important information	1	2	3	4	5
11	Employees are free to report their issues of concern to anyone regardless of position in the organisation	1	2	3	4	5
12	My organisation provides general induction (training) to new employees	1	2	3	4	5

13	Employees normally share information on critical issues in my organisation	1	2	3	4	5
Information Security Training						
	Please rate the following statements:	**Not at all 1**	**Little 2**	**Average 3**	**More than Average 4**	**A lot 5**
14	My organisation has an information security awareness training programme	1	2	3	4	5
15	IT officers in my organisation are trained on how to respond to information security matters	1	2	3	4	5
16	My organisation provides ongoing refresher courses/training on information security	1	2	3	4	5
17	Training on information security awareness is important for my organisation	1	2	3	4	5
18	Most employees (who use computers) in my organisation have received information security awareness training	1	2	3	4	5
Cybercrime Reporting						
19	I always report cybercrime incidents that I experience	1	2	3	4	5
20	I know where to report cybercrime incidents in my organisation	1	2	3	4	5
21	The IT department/unit in my organisation understands what to do about reported cybercrime incidents	1	2	3	4	5
22	I think most cybercrime incidents are reported in my organisation	1	2	3	4	5
23	I know that it is important to report cybercrime incidents in my organisation	1	2	3	4	5

24	How experienced are you in using computers?	**Poor 1**	**Little 2**	**Average 3**	**Very good 4**	**Excellent 5**

Additional Comments

Thank you for taking the time to respond to this questionnaire.

Appendix D: Questionnaire Items Descriptive Statistics

Variable	Descriptive Statistics				
	Valid N	Mean	Minimum	Maximum	Std.Dev.
AWARE1	54	1.814815	1.000000	5.000000	0.870352
AWARE2	54	1.592593	1.000000	4.000000	0.630020
AWARE3	54	1.574074	1.000000	3.000000	0.601942
AWARE4	54	1.611111	1.000000	3.000000	0.596109
LEGIS1	54	1.592593	1.000000	4.000000	0.714236
LEGIS2	54	1.388889	1.000000	2.000000	0.492076
LEGIS3	54	1.481481	1.000000	4.000000	0.693385
LEGIS4	54	1.444444	1.000000	3.000000	0.537874
CULTR1	54	2.481481	1.000000	4.000000	0.693385
CULTR2	54	2.425926	1.000000	3.000000	0.569735
CULTR3	54	4.129630	3.000000	5.000000	0.753515
CULTR4	54	3.814815	1.000000	5.000000	0.802686
CULTR5	54	3.407407	1.000000	5.000000	1.173907
TRAIN1	54	1.500000	1.000000	4.000000	0.606568
TRAIN2	54	1.407407	1.000000	2.000000	0.495966
TRAIN3	54	1.407407	1.000000	3.000000	0.532652
TRAIN4	54	1.537037	1.000000	5.000000	0.770027
TRAIN5	54	1.574074	1.000000	3.000000	0.632511
REPOT1	54	1.388889	1.000000	3.000000	0.596109
REPOT2	54	1.462963	1.000000	4.000000	0.719354
REPOT3	54	1.500000	1.000000	5.000000	0.795032
REPOT4	54	1.500000	1.000000	3.000000	0.574620
REPOT5	54	1.370370	1.000000	3.000000	0.559525

Appendix E: Factor Analysis (0.55 value & 5 factors)

Showing all items

Factor Loadings (Varimax normalized) Extraction: Principal components (Marked loadings are >.550000)					
Variables	**Factor 1**	**Factor 2**	**Factor 3**	**Factor 4**	**Factor 5**
AWARE1	-0.008678	0.842051	0.074911	0.257815	-0.005544
AWARE2	0.145255	0.863327	-0.001517	-0.110352	0.023135
AWARE3	-0.059521	0.769254	0.105322	-0.019758	0.046728
AWARE4	0.158326	0.680171	-0.000829	-0.035861	0.023754
LEGIS1	0.008674	-0.082097	0.819750	0.178395	-0.124836
LEGIS2	-0.078436	0.181238	0.695558	0.130474	0.084924
LEGIS3	0.109304	0.022795	0.783965	0.130144	-0.118895
LEGIS4	-0.089738	0.065868	0.839818	-0.014977	0.102297
CULTR1	0.177348	0.280073	0.279051	-0.071051	0.247552
CULTR2	-0.026051	0.347787	0.112436	-0.063154	0.615359
CULTR3	0.036489	-0.044116	0.046769	0.113937	0.809004
CULTR4	-0.062990	0.115334	-0.019285	-0.055725	0.785897
CULTR5	-0.018215	0.179117	0.144719	-0.107223	-0.503267
TRAIN1	0.443997	-0.040387	0.038434	0.791371	0.081937
TRAIN2	-0.019607	0.027548	0.167875	0.832947	0.004772
TRAIN3	0.116729	0.028427	0.195533	0.867555	0.052054
TRAIN4	0.044757	-0.031753	0.028850	0.701890	0.016718
TRAIN5	0.511691	0.075960	-0.080175	0.549930	-0.013455
REPOT1	0.831764	0.158219	0.018602	0.274030	0.027785
REPOT2	0.795239	0.275213	-0.161277	0.162203	0.048307
REPOT3	0.701893	0.016268	0.325791	-0.071687	-0.134699
REPOT4	0.566906	-0.378850	0.367662	-0.128479	0.050601
REPOT5	0.607170	0.003331	-0.201541	0.174649	0.011903

Appendix F: Construct Item Analysis

Cybercrime Awareness (AWARENESS)

Summary for scale: Mean=7.03704 Std.Dv.=2.14531 Valid N:54 Cronbach alpha: .825185 Standardized alpha: .833992 Average inter-item corr.: .568052					
Items	Mean if (deleted)	Var. if (deleted)	StDv. if (deleted)	Itm-Totl (Correl.)	Alpha if (deleted)
AWARE1	5.092593	2.046982	1.430728	0.721607	0.765455
AWARE2	5.314815	2.623114	1.619603	0.807790	0.714995
AWARE3	5.351852	3.042867	1.744382	0.575326	0.812465
AWARE4	5.351852	3.042867	1.744382	0.575326	0.812465

Understanding of Cybercrime Legislation (LEGISLATION)

Summary for scale: Mean=6.05556 Std.Dv.=2.06879 Valid N:54 Cronbach alpha: .827061 Standardized alpha: .829945 Average inter-item corr.: .554630					
Items	Mean if (deleted)	Var. if (deleted)	StDv. if (deleted)	Itm-Totl (Correl.)	Alpha if (deleted)
LEGIS1	4.407407	2.130316	1.459560	0.731365	0.746136
LEGIS2	4.666667	2.925926	1.710534	0.557720	0.823136
LEGIS3	4.555555	2.358025	1.535586	0.649323	0.785777
LEGIS4	4.537037	2.581962	1.606848	0.708186	0.761456

Organisational Culture (O_CULTURE)

Showing only 4 Items (CULTR5 deleted)

Summary for scale: Mean=9.01852 Std.Dv.=1.89827 Valid N:54 Cronbach alpha: .627040 Standardized alpha: .639187 Average inter-item corr.: .311729					
Items	Mean if (deleted)	Var. if (deleted)	StDv. if (deleted)	Itm-Totl (Correl.)	Alpha if (deleted)
CULTR1	6.518518	2.545954	1.595604	0.263898	0.652613
CULTR2	6.555555	2.506173	1.583090	0.495264	0.527504
CULTR3	7.148148	2.126200	1.458150	0.391920	0.571452
CULTR4	6.833333	1.768519	1.329857	0.537009	0.447353

User Training on Information Security Awareness (TRAINING)

Summary for scale: Mean=7.20370 Std.Dv.=2.35828 Valid N:54 Cronbach alpha: .838569 Standardized alpha: .853297 Average inter-item corr.: .555935					
Items	Mean if (deleted)	Var. if (deleted)	StDv. if (deleted)	Itm-Totl (Correl.)	Alpha if (deleted)
TRAIN1	5.740741	3.340192	1.827619	0.802141	0.759754
TRAIN2	5.814815	3.965706	1.991408	0.646443	0.809178
TRAIN3	5.870370	3.668381	1.915302	0.784878	0.774547
TRAIN4	5.740741	3.414266	1.847773	0.549599	0.844516
TRAIN5	5.648148	3.783608	1.945150	0.523406	0.839421

Cybercrime Reporting (REPORTING)

Summary for scale: Mean=7.22222 Std.Dv.=2.35257 Valid N:54 Cronbach alpha: .764836 Standardized alpha: .765463 Average inter-item corr.: .438921					
Items	Mean if (deleted)	Var. if (deleted)	StDv. if (deleted)	Itm-Totl (Correl.)	Alpha if (deleted)
REPOT1	5.833333	3.435185	1.853425	0.752878	0.650361
REPOT2	5.759259	3.256859	1.804677	0.648208	0.678109
REPOT3	5.722222	3.274691	1.809611	0.539192	0.727476
REPOT4	5.722222	4.237654	2.058556	0.371355	0.771924
REPOT5	5.851852	4.200274	2.049457	0.406915	0.761594