UNIVERSITY OF KWAZULU-NATAL

PERSONAL INFORMATION SECURITY: LEGISLATION, AWARENESS AND ATTITUDE

By

Steven Parbanath

210555757

A thesis submitted in fulfilment of the requirement for the degree of Master of Commerce

School of Management, IT & Governance

College of Law & Management Studies

Supervisor: Prof. Manoj S. Maharaj

2011

Supervisor's permission to submit for examination

Date: _____

Student Name: S. Parbanath

Student number: 210555757

Dissertation Title: Personal information security: Legislation, Awareness and Attitude

As the candidate's supervisor I agree to the submission of this dissertation for examination. **To the best of my knowledge, the dissertation is primarily the student's own work and the student has acknowledged all reference sources.**

The above student has also satisfied the requirements of English language competency.

Name of Supervisor: Professor Manoj S. Maharaj

Signature: _____

DECLARATION

I, Steven Parbanath, declare that

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

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

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

(iv) This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers.
Where other written sources have been quoted, then:
a) Their words have been we-written but the general information attributed to them has been referenced.
b) Where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

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

Signed: .....

ACKNOWLEDGEMENTS

I wish to express my sincere appreciation to all those who contributed to this study.

In particular, I would like to thank the following persons:

- Professor Manoj S. Maharaj, my supervisor, for his professional guidance.
- Mr Deepak Singh for his assistance with the statistical analysis.
- The library staff at the Riverside campus (PMB) for their services.
- The staff at Durban University of Technology who filled out the questionnaire for the research.

S. Parbanath

Durban

2011

ABSTRACT

Ecommerce refers to the buying and selling of products and services electronically via the Internet and other computer networks (Electronic Commerce 2011). The critical components of ecommerce are a well designed website and a merchant account for payment by the customer (Ecommerce critical components 2008). Merchants that sell their products and services via the Internet have a competitive edge over those that do not. It is therefore becoming common practice for both small and large business to transact electronically. With the vast opportunities, new risks and vulnerabilities are introduced. Consumers are reluctant to transact electronically because of the fear of unauthorized access and interception of confidential information (Online Banking Concerns 2011). Other fears include the changing of data with malicious intent, denial of use, hacking, deliberate disclosure of confidential information and e-mail associated risks (Safeena, Abdulla & Date 2010). The use of technology such as encryption and decryption has not adequately addressed these problems because fraudsters have found new and sophisticated methods of attaining consumer information illegally. Phishing is one such method. Phishing results in identity theft and financial fraud when the fraudster tricks the online users into giving their confidential information like passwords, identity numbers, credit card number and personal information such as birthdates and maiden names. The fraudster will then use the information to impersonate the victim to transfer funds from the victim's account or use the victim's information to make purchases (Srivastava 2007). Since 2002, many laws passed in South Africa have attempted to allay fears so that consumers can conduct business electronically with confidence. The following legislation aims to protect consumers:

- The Electronic Communications and Transactions Act (Republic of South Africa 2002).
- The Consumer Protection Act (Republic of South Africa 2008).
- The Protection of Personal Information Bill which is expected to be passed in 2011 (Republic of South Africa 2009).

This research aims to examine the extent to which these legislation can address the security concerns of consumers. The researcher is also interested in ascertaining how knowledgeable consumers are on these legislation and what their attitudes are towards their personal information security.

CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXURES

Chapter One

1. BACKGROUND AND CONTEXT

1.1 Introduction

Business requires confidential and personal information from customers. The identity number, passwords, credit card number and birthdates are examples of personal and confidential information. This type of information is generally referred to as Personal Identifiable Information (PII). This Personal Identifiable Information (PII) is required when customers make an application for credit and shopping cards or when a hire purchase agreement is signed with an enterprise. Personal Identifiable Information is also required when customers shop on-line. Customers are concerned about the security of this information (Online Banking Concerns 2011). The areas of concern are (Castaneda, Montoso & Luque 2007):

- Collection of the information (referred to as "collect").
- Use of the information (referred to as "use").
- Online transactions.

The dimension "collect" relates to how safe the information is with the data collector after it has been collected from the consumer. The dimension "use" relates to whether the information that is collected is used for the intended purpose only. Customers are also concerned about the security of their PII when transacting online because personal information can be stolen and used illegally on the Internet (Online Banking Concerns 2011). Legislation has been put in place to address these concerns. The Electronic Communications and Transactions Act of 2002, The Consumer Protection Act of 2008 and The Protection of Personal Information Bill of 2009 (this Bill is expected to become an Act of Parliament in 2011) are examples of legislations that have been formulated to protect the consumer. Legislation may lead to customers transacting with more confidence and thereby increasing e-commerce activities.

1.2 The Internet Security Problem

This section deals with a variety of problems that are being experienced with regard to electronic transactions and communication.

1.2.1 New Risks and Vulnerabilities

One of the major reasons why there is a fear to conduct business electronically is the Internet Security Problem (Malhotra, Kim & Agarwal 2004). Escalating Internet vulnerabilities and risks, combined with an absence of adequate regulation at levels ranging from organizational through to global have led to concerns regarding the personal information security of customers (Jamieson *et al*. 2008). The Internet's evolving and dynamic nature continues to reveal new risks and vulnerabilities.

1.2.2 The Problems relating to Electronic Business

Some of the problems relating to electronic business conducted through the Internet are:

- Businesses bordering closely on infringing on domain names. Domain names are divided into hierarchies. In "microsoft.com" for example, "com" is the first level while "Microsoft" is the second level in the hierarchy. Problems arise when two enterprises decide to have identical first and second level domain names. Problems may also occur when the second level domain names of two enterprises are similar. This will result in disputes when trademarks and other traditional business identifiers are used (Mohan 2011).
- Credit card information is stolen and used illegally on the Internet. The most common methods used are identity theft and stolen credit card numbers (Romanosky, Telang & Acquisti 2008).
- Personal information is sent in clear, unencrypted text allowing others to gain access for criminal use. Criminals can intercept unencrypted text and attachments from the Internet (Information Security 2011).
- Internet Service Providers (ISPs) and business sites are hacked and changed. A hacker is an intruder with malicious intent. This malicious intent includes stealing (AlAwadhi and Moris 2009)
    1. Customers' personal information.
    2. Credit card details for identity theft.

3. Passwords for illegal access to online banks, Internet Service Providers (ISPs) or web services.
4. Email addresses so that unsolicited emails (Spam) may be sent (Castaneda *et al.* 2007).

- Internet hardware and software are vulnerable to numerous types of attacks by anyone in the world. To prevent this, a firewall is normally installed. A firewall has a single checkpoint through which all incoming and outgoing data is controlled. The firewall therefore acts as a guard which identifies each packet of information that may pass through (Firewalls 2011). The problem is that small businesses are most vulnerable to attacks because they cannot afford to invest in firewalls (Firewalls 2011). Firewalls are however expensive to install and maintain. Hackers know this and they will therefore target small business.
- Denial of service attack. A denial-of-service attack attempts to make computer resources unavailable for customers to use. The aim of the perpetrator is to prevent the efficient functioning of the Internet and as a result, customers are prevented from executing their online transactions. The main targets are banks and credit card payments gateways (Shahzad, Naseem, Aadil & Khayyam 2010).

1.2.3 Internet Risks

There are numerous possible Internet risks which hamper or deter consumers from conducting business electronically. Commercial Internet use has resulted in the interception of data in transit by competitors or criminals. Hacking of sensitive corporate databases that contain information about customers is common (What are the effects of Computer Hacking? 2010). Customers are concerned that disgruntled employees and ex-employees can disclose, alter or delete their personal information (Castaneda *et al.* 2007). Customers' personal information can also be compromised when the Internet is used for non-business purposes (Aaron 2010). One such example is contained in an article which appeared in the Daily Dispatch on 25 April 2010 (Stone 2010). The article relates to an incident where an Internet user accidently stumbled across a file containing patient's information while searching Google. The files contained personal information of around 20000 patients from provincial hospitals in the Western Cape (Stone 2010). Erroneous online transactions also contribute to customers' concerns regarding their personal information security (Aaron 2010). Customers are also concerned that viruses can be deliberately sent and these can take the form of infection from files attached to messages (Zimerman 2011). These viruses can alter or delete

the information in their databases (What are the effects of Computer Hacking? 2010). Unauthorized disclosure of sensitive information can result from emails. This can take the form of the deliberate export of sensitive information as well as the interception of outgoing messages. Customers are concerned that this information is accessed or received by someone other than the intended recipient (What are the effects of Computer Hacking? 2010). Spam is another source of privacy invasion. Spam (also referred to as junk mail) is defined as an inappropriate use of a mailing list. This may involve the sending of advertisements or messages to a large number of people that did not request for these. Spam has become illegal in many countries, especially in the European Union (Castaneda *et al.* 2007). Another concern is that the Internet can be used to defame an individual or organization. Defamation consists of false publications that may result in economic damages.

These Internet risks have to be addressed so that customers will embrace technology without being concerned about their personal information being compromised.

1.3 Identity Theft

Identity theft is broadly defined as a crime whereby the criminal gains access to the Personal Identifiable Information (such as passwords, birthdates and maiden name) of a victim. The perpetrator will then use this information to impersonate the victim and carry out fraudulent activities like withdraw funds from the victim's account or make fraudulent purchases on the Internet (Srivastava 2007).

There are two categories of identity theft (Reducing the Risk of Identity Theft 2010). The first category is referred to as common identity theft and the second category is called Internet identity theft. In common identity theft, the perpetrator can obtain the victim's personal information without using any technological means such as the Internet. Common identity theft can take place in the following manner (Reducing the Risk of Identity Theft 2010):

- The theft of a wallet which contains a credit or ID card.
- The fraudster asks the victim for his or her personal information.
- The perpetrator asks a third party for the victim's personal information.
- The fraudster acquires the personal information by reading a financial statement (such as a bank statement) of the victim.

The second category (Internet identity theft) involves the perpetrator using more sophisticated methods of stealing an individual's personal information on the Internet. This may involve the interception of the victim's personal information or using sophisticated methods like phishing and pharming (Anderson, Durbin & Salinger 2008). Phishing result in identity theft and financial fraud when the fraudster tricks the online users into giving their confidential information like passwords, identity numbers, credit card number and personal information such as birthdates and maiden names (Aaron 2010). Pharming attacks redirect online users from legitimate websites to fraudulent ones (Brody, Mulig & Kimball 2007). The fraudulent website looks exactly like the legitimate one. Users will interact with the fraudulent website and disclose their personal information on this website thinking it is the legitimate one. The perpetrator can then get the personal information of the customer from the fraudulent website and use it illegally (Pharming 2011).

A perpetrator can use a victim's personal information as follows:

- Account takeover: In this case the perpetrator will use the victim's personal information to make fraudulent purchases by using the actual credit card or using the credit card number. The victim generally learns that his account has been taken over by the perpetrator when he notices discrepancies in his monthly statements (Siciliano 2011).
- Application fraud: In this case, the perpetrator will use the victim's personal information to open a new account in the victims' name. The monthly statements are mailed to the perpetrator's address and therefore it becomes difficult to discover the theft for some time (Fraud: awareness and prevention 2011).

Phishing has now become the most common method of identity fraud (Nwaocha 2010). The RSA Anti-Fraud Command Centre provides some statistics regarding phishing attacks. There is generally around 15000-18000 phishing attacks worldwide every year. Since September 2010 there has, however, been a slight decrease. In 2010, 65% of attacks were directed at national banks, 30% of attacks are directed at regional banks and about 5% target credit unions. The United States is the biggest target with 37% of attacks. The UK is second with 27% followed by South Africa with 15%. China experienced 7% of attacks and Italy 3% (Aaron 2010).

For more statistics on identity fraud, the researcher decided to use the results of two studies conducted in the United Kingdom. These studies were conducted by companies that

specialize in fraud and identity protection. These UK based studies are used because the researcher could not find statistics on identity fraud regarding the South African consumer. The purpose of using statistics is to show that identity fraud is a major contributor to the Internet Security Problem (Aaron 2010). The results of the first study show that identity theft is a serious concern to customers. The results of the second study show that customers themselves are partly to blame for an increase in identity theft.

The first study was conducted by Lloyds TSB in 2009. The aim of the research was to collect information on customers' feelings, concerns and attitudes regarding identity theft. The results show the following (Identity Theft Expert 2009):

- 76% of adults are concerned about identity theft.
- 39% feel more at risk now than they did before the recession (i.e. before 2008).
- 52% of those concerned feel that the recession has increased the cases of identity theft.
- 57% of people believe that social networking sites have increased the incidences of identity theft.
- 38% have experienced identity theft and 18% have already become victims.
- 57% admit that they have not done enough to protect themselves.
- 25% do not know how to protect themselves against identity theft.

The second research was carried out by Sophos. The aim of this experiment was to determine how responsible the British public is towards their personal information security. They randomly asked people in Bristol for personal information like their names, e-mail address, maiden name and date of birth. All but one disclosed this information. The experiment indicates that people were oblivious to the fact that they were disclosing their personal information which could be used to carry out Internet associated crimes. The researcher concludes by stating that the public can reduce identity theft by not disclosing any personal information to strangers (Identity Theft Expert 2009).

1.4 Research objectives

This research investigates:

- How legislation addresses consumer concerns regarding their personal information security.

- Customers' attitudes towards their personal information security.
- The level of knowledge consumers have regarding their personal information security.

1.5 Rationale for the study

The researcher has done many searches of completed theses and dissertations to determine whether a similar study has been carried out in a South African context. The NRF database was also thoroughly searched. The researcher is therefore convinced that there is no study conducted that investigates how legislation can addresses customers' concerns on personal information security (in a South African context). Further, the researcher could not find any published articles relating to customers knowledge and attitudes regarding their personal information protection (in a South African context). It is therefore important to conduct this research to meet the objectives indicated in 1.4.

By publishing the results of the study in reputable magazines, consumers will become more educated about their rights. Education will empower customers to question companies about their (the consumer's) personal information security. Education will also lead to customers taking the appropriate course of action if their personal information has been compromised (Romanosky, Telang & Acquisti 2008). One such action is reporting violations to the National Regulator (The Protection of Personal Information Bill 2009). Awareness and education may lead to customers willingly surrendering their personal information with the knowledge that they are protected by legislation.

1.6 Limitations of the study

1.6.1 The Protection of Personal Information Bill of 2009 is expected to become an Act of Parliament in 2011 and customers may be unaware about this new proposed legislation.

1.6.2 The main focus of the study is on how personal information security issues of the South African consumer can be addressed. Statistical information was required to show that identity fraud is of serious concern to the customer. The researcher however could not find similar studies in a South African context where statistics were available. The researcher therefore had to refer to studies carried out in the United Kingdom and the United States of America for such information.

1.7 Conclusion

This chapter puts the entire study into context by focussing on the Internet Security Problem, research objectives, rationale for the study and limitations of the study.

1.8 Outline of chapters

The study is broken down into the following chapters:

Chapter 1 deals with the background of the study, the Internet Security Problem, the research objectives, the rationale of the study and the limitations of the study.

Chapter 2 deals with the literature review that supports the study for a motivation as to why this investigation is important.

Chapter 3 deals with the research questions to be answered, the theoretical framework and the research methodology used in the study.

Chapter 4 provides the results of the research in a manner that is easy to interpret. An analysis of the results is then done.

Chapter 5 focuses on the conclusion of the study with recommendations.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

The Government has introduced legislation as an important strategy to address the Internet Security Problem. This study therefore focuses on the Electronic Communications and Transactions Act (Republic of South Africa 2002), the Consumer Protection Act (Republic of South Africa 2008) and the Protection of Personal Information Bill (Republic of South Africa 2009). According to the Protection of Personal Information Bill (Republic of South Africa 2009), legislation regarding the personal information security of the customer is important for the following two reasons:

- To provide confidence to consumers that their personal information is safe in the hands of business;
- To provide a platform for customers to take the necessary steps when they become victims of identity theft. In such a case, the National Regulator will have to be informed so that the necessary legislative processes are followed.

Since computer ethics and fraud have become a global phenomenon, personal information protection in the USA and the EU is also examined. These regions are chosen because they were the first to pass legislation regarding personal information protection (Data Protection Directive 2011). The researcher focuses specifically on the 95/46/EU directive (also referred to as the Data Privacy Directive). This directive specifically aims to strike a balance between the high level of protection for the privacy of individuals and the free movement of personal data within the EU. The 95/46/EU directive does not consider the transfer of information outside the EU. The researcher also focuses on the „U.S Safe Harbor' agreement which aims to extend the 95/46/EU directive. This agreement allows personal information to be transferred from the EU to the United States and vice versa. The role the International Criminal Police Organization (INTERPOL) plays in combating cybercrimes is also considered.

According to Romanosky *et al* (2008: 5), a data breach is generally considered "an unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data that compromises the security, confidentiality, or integrity of personal information." Types of personal information include name, date of birth, passport ID,

biometric or other kinds of personally identifiable data. Biometrics is defined as a biological identification of a person such as fingerprint, retinal patterns and voice (TechWeb 2007).

According to Romanosky *et al*. (2008) there are a number of ways a company can become aware of a data breach. Firstly, they may detect it themselves. Secondly, they may be notified by the customer who notices that his or her personal information has become public knowledge. Thirdly, the customer may notice in his or her financial statements that some irregular activities has taken place and then notify the company of such irregularities.

There is certainly a motivation for legislation to assist in reducing the level of identity theft. Firstly, by having these laws, companies will become aware of the consequences of data breaches. They will then become proactive in improving their internal security controls even if they have not been breached previously (Ranger 2007). They will also make the effort to send notification letters to customers when a breach has taken place. Companies will also be motivated to embark on educational campaigns and monitoring activities.

Secondly, customers feel that they have a right to be informed when companies use or abuse their information (Romanosky *et al*. 2008). Having been informed of a breach, a customer will be in a position to take appropriate action. One such action would be to request a banking institution to freeze an account. With knowledge and awareness of consumer protection legislation, customers can engage the services of a law enforcement agency such as the SAPS or have the recourse of the National Regulator who will then decide whether to prosecute or not.

2.2 A conceptual model: The impact of legislation on identity theft

Figure 2-1 outlines the conceptual model which highlights the impact of legislation on identity theft in the United States of America. The primary effect of data breach disclosure laws is for business to notify customers when a breach has taken place. Notifying customers of a data breach is mandatory in the United States of America (Romanosky *et al*. 2008). Once customers are notified, they will take precautionary measures. As more affected customers are notified, more will take precautionary measures and the net result is a reduction in identity theft.

Sending notifications to affected customers is costly. Not only will the company suffer financially, but the reputation of the company also suffers (Ranger 2007). To avoid this, companies will become motivated to introduce strategies to limit identity theft. This is the

secondary effect of legislation (see figure 2-1). The incentive for companies is to improve their security controls so that the cost of notifying affected customers and the loss of reputation is avoided. It has been shown that customers lose confidence in a company that suffers breaches (Romanosky *et al*. 2008). It is therefore in the interest of companies to improve their security measures in order to regain customer confidence.

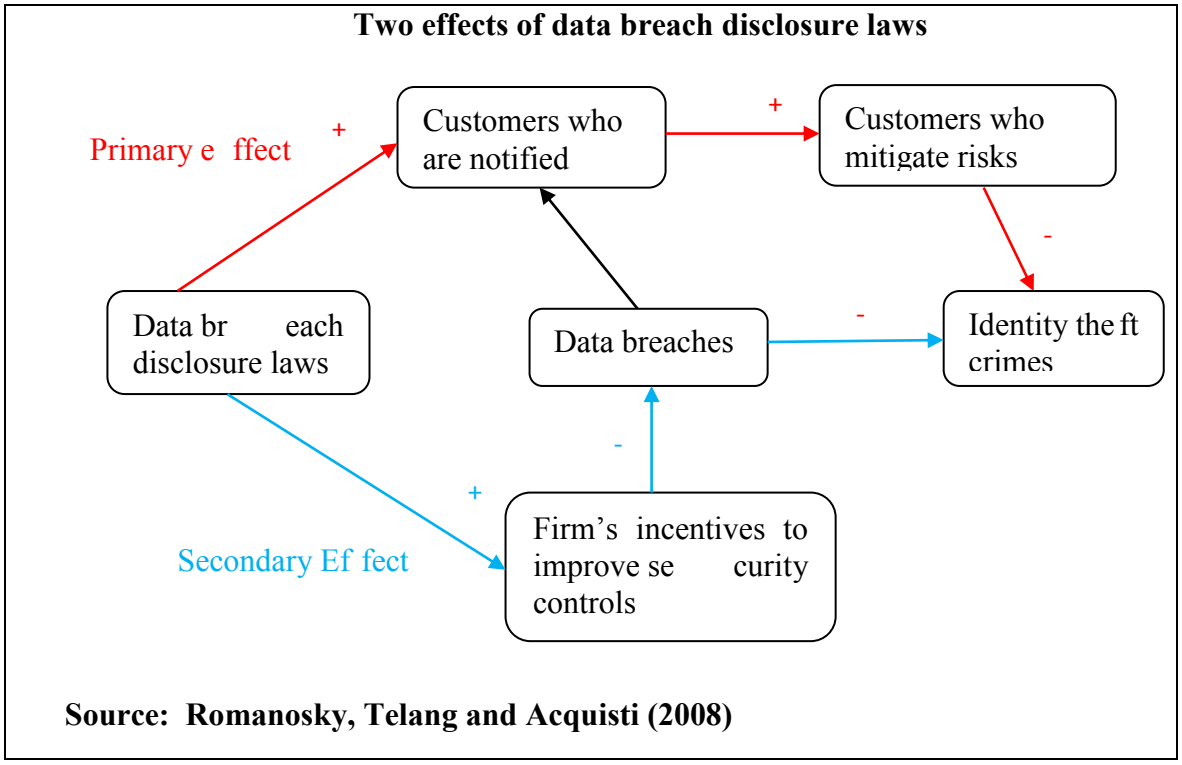


Figure 2-1: Two effects of data breach disclosure laws

2.3 Privacy invasion and legislation in a global context

This section deals with the common ways an individual's privacy can be violated and how global legislation aims to minimize this. Since data protection legislation in South Africa is formulated using the legislation of the European Union, a comparative study is made between the 95/46/EC directive of the European Union and legislations in South Africa. A comparison is also made between the 95/46/EC directive of the European Union and the "Safe Harbor" agreement of the United States.

The Directive 95/46/EC of the European Parliament encourages the exchange of information between countries in Europe for e-commerce development and advancement. The aim of data protection legislation in South Africa is to encourage customers to surrender their personal information to business so that ecommerce activity is increased (The Electronic Communications and Transactions Act 2002). During the exchange of information, the

fundamental rights of consumers should be safeguarded. This means that the customers' personal information should not be violated. Any violations in this regard can lead to a criminal prosecution (Data Protection Directive 2011).

The 95/46/EC Directive and the Electronic Communications and Transactions Act of South Africa define a "data subject" as a person from whom the data is collected. A "data controller" is defined as a person or organization that has in its possession the data of the data subject. An example of a data subject is a customer and an example of a data controller is a business enterprise.

The 95/46/EC has basic principles that an enterprise should adhere to. These basic principles are compared to the basic principles enshrined in South African data protection legislation. In other words, the rights of a data subject in the EU and rights of the data subject in South Africa are compared.

- Both the 95/46/EC directive and the Protection of Personal Information Bill of 2009 give the right to the data subject to know who the data controller is, the purpose for which the data was collected and who the third party recipients of the data are (Data Protection Directive 2011).
- The data subjects in the EU and South Africa can object to the data being used for direct marketing. This means that permission must be sought from the data subject before his or her personal information is used for direct marketing. With regard to direct marketing, the data subject in South Africa has more rights than the data subject in the EU. The data subject in South Africa has the right to know the identity of the sender while the 95/46/EC directive does not make mention of this. If direct marketing is not involved, then minimal processing can be done without seeking the permission of the data subject (in a South African context). This could take the form of statistical analysis such as determining trends and marketing research. (Protection of Personal Information Bill 2009). The EU, however, does not have such provisions in its legislations (Privacy and Human Rights 2003: Overview 2003).
- The data subjects in the EU and South Africa have the right to view the data in its entirety as well as correct and erase sections of the data that is incorrect or inconsistent. The Protection of Personal Information Bill of South Africa, however, goes one step further by giving a customer the right to stop any processing of the data

provided the data controller has reasonable grounds to do so. The 95/46/EC directive has no such provisions (Privacy and Human Rights 2003: Overview 2003).

- The 95/46/EC directive states that the data collected should be used for a specified reason and no other. The Protection of Personal Information Bill of South Africa allows for further processing of data. This means that not only can the data be used for the original purpose, but it can also be used to do other processing provided it is related to the original purpose. Permission must also be given by the data subject for further processing to take place (Protection of Personal Information Bill 2009).

Legislation in both the EU and South Africa has put the onus on the data controller to be solely responsible for the security of the data of the data subject. The data controller must take appropriate steps to ensure the security of the data (Protection of Personal Information Bill 2009).

The European Union has made Spam a criminal offence. Countries that belong to the European Union in particular have strong legislation regarding the sending of unsolicited emails (Castaneda *et al*. 2007). There are however loopholes that can be violated. In such cases, it is left to an individual to file a claim or apply technological solutions to counteract this. One technological solution could be to apply filtering procedures that will reject Spam (Castaneda *et al*. 2007). Spam is not illegal in South Africa. Customers do receive unsolicited emails from enterprises although they (customers) may be against it. However, the processing of personal information of a data subject for direct marketing using Spam is illegal unless consent has been given by the customer (Protection of Personal Information Bill 2009).

Although the Internet is used mainly to promote e-commerce, it can be used illegally as "word of mouth" to defame an organization or individuals. This can take the form of false information being circulated about an individual or company. This could lead to loss of revenue by an organization. As a consequence, the European Union Court of Justice has ruled that it is illegal to post a person's image, video or personal information on the Internet without consent being granted by the person concerned (Castaneda *et al*. 2007). Data protection legislation in South Africa does not have any sections regarding the posting of an individual or organization image, video or personal information on the Internet. Data protection legislation in South Africa, however, aims to protect a customer when personal

information is surrendered to business for the purpose of carrying out a transaction (Protection of Personal Information Bill 2009).

Another practice is that companies use customer information without authorization to create huge databases. This is done by recording customer navigation details or by asking customers questions and carrying out surveys (Privacy and Human Rights 2003: Overview 2003). In the former instance, websites may have a lot of information about the user because servers record information about the users browsing habits. According to the European Parliament, recording and storing this information without authorization from the customer is illegal since it constitutes an invasion of privacy. Also, the sharing or selling of this information without authorization from the customer is also illegal (Data Protection Directive 2011). South African legislation, however, does not have a specific section regarding unauthorized browsing and recording of a customer's data (The Protection of Personal Information Bill 2009).

The United States approach to personal information protection is regional and self-regulatory (Data Protection Directive 2011). This means that each state in the United States have their own legislation relating to personal information protection. The EU found such an approach undesirable since it lacks uniformity. The EU was therefore concerned about the safety of personal data when transmitted to the US. This discrepancy between the approach adopted by the EU (strong legislation between member countries) and the approach adopted by the US (self-regulatory) led to the negotiation of a „Safe Harbor' agreement to ensure the continued trans-border flow of information between the EU and the US and vice versa. The idea was that US companies would adhere to the principles worked out by the United States Department of Commerce and the Internal Market Directorate of the European Commission. This created the presumption for US companies that the legislation was adequate to continue receiving personal data from the EU (Privacy and Human Rights 2003: Overview 2003).

The general principles enshrined by the "Safe Harbor" agreement are similar to the general principles of the Protection of Personal Information Bill of 2009 (South African Legislation) and the general principles of the 95/46/EC directive (European Legislation). These principles are as follows (Data Protection Directive 2011):

- All signatory organizations to the "Safe Harbor" agreement must provide clear notice as to the kind of information that is to be collected, the purpose for which it may be used and any third parties that may require the information.

- Individuals must be given the ability to choose what data to provide to an organization.
- Individuals should also be given the chance opt out if they do not wish to disclose their personal information.
- An organization can disclose personal data to a third party if it (the third party) is a signatory to the „Safe Harbor' agreement or if the third party signs to protect the data.
- Organizations must take steps to protect the data.
- Individuals must be allowed to change, amend or delete data that is inaccurate.
- Organizations that collect data must have mechanisms that may carry out investigations and provide compensation when violations have taken place (Kyl 2000).

The 95/46/EC Directive deals with the protection of data within the European Union (between member countries in Europe) while the „Safe Harbor' agreements deal with protection of personal information when transferred from Europe to the United States and vice versa (Data Protection Directive 2011). There is, however legislation that has been passed that deals specifically with identity theft within the United States. In 1998, the US Congress passed the Identity Theft and Assumption Deterrence Act (18 USC 1028) which makes identity theft a federal felony (Jamieson *et al*. 2008). The Identity Theft Penalty Enhancement Act of 2004 was passed in the United States to enhance the Theft and Assumption Deterrence Act of 1998. The Anti-Phishing Act passed in 2004 aims to protect users against this crime (Laws that protect the internet from phishing, Congress and Phishing 2004). Cybercrimes are prosecuted by the US Department of Justice (Cassim 2009).

Since ecommerce activity is now a global phenomenon, the security of personal information across borders is paramount. The International Criminal Police Organization (INTERPOL) facilitates the protection of information across borders (Jamieson *et al*. 2008).

2.4 Inter-Jurisdictional Legislation

The International Criminal Police Organization (INTERPOL) is an organization that facilitates law enforcements between member countries. Countries who are members of INTERPOL have access to databases containing criminal information. This enables member countries to communicate with each other to enhance international police cooperation (Jamieson *et al*. 2008).

Since cybercrime is an international problem, INTERPOL will collect, store, analyse and share information among the 186 member countries through its global police communication system. INTERPOL's cybercrime programmes are designed to (Jamieson *et al*. 2008):

- Facilitate cooperation between member countries around the clock to monitor cybercrimes.
- Increase the exchange of information between member countries on the operations of perpetrators.
- Assist member countries in the event of a cyber attack.
- Develop strategic partnerships with other international organizations and the private sector.

In addition to having INTERPOL as an international police body to help investigate cyber crimes, The Convention on Cyber Crime of the Council of Europe was formed in 2004. The Convention contains the definitions of different types of cyber crimes and lays the foundation for legislation to be adopted by countries of the European Union to deal with cyber crimes (Jamieson *et al*. 2008).

2.5 The Electronic Communications and Transactions Act of June 2002 (ECT)

Although this legislation seems old (i.e. 2002) in an IT context, it is important to focus on a few critical aspects from this Act. Where possible, a comparison of this legislation is made with the European Union Legislation on personal information security known as the 95/46/EC directive. The Electronic Communications and Transactions Act 2002 is an important Act for the following two reasons:

- Firstly, for the first time legislation has made it possible for an individual to be prosecuted if found guilty of committing a cybercrime (Cassim 2009).
- Secondly, this Act made it possible for subsequent legislations relating to information security to be passed in parliament. It therefore formed the cornerstone for many important IT related legislations to follow.

The purpose of this section is to therefore provide a brief background of the contents of the Act. Only those parts of the Act which pertain to the promotion of consumer protection, electronic communication and transaction, fraud and ethics are considered.

2.5.1 The objectives of the Act

The main objectives are encapsulated as follows (Electronic Communications and Transactions Act 2002: 8):

- "To enable and facilitate electronic communications and transactions in the public interest."
- "To promote e-commerce."
- "To develop a safe, secure and effective environment for e-commerce."

2.5.2 Protection of personal information

The broad principles of the Electronic Communications and Transactions Act of 2002 are based on the principles of data protection legislation of the European parliament known as the 95/46/EC directive (The Electronic Communications and Transactions Act 2002). A comparison between the 95/46/EC directive and general data protection legislation in South Africa has already been made in section 2.3. The Electronic Communications and Transactions Act of 2002 have however, additional principles not contained in the 95/46/EC directive. These are (Hofmeyr 2011):

- The data collector can keep the data for a period of one year after having used the data.
- The information collected may not be given to a third party unless required by the law.
- If the personal information was required legally to be given to a third person, then the data controller must keep a record of this. The information that should be kept is the date it was disclosed to the third person and the purpose for which the data was required.
- All obsolete information must be deleted by the data controller.
- The organization controlling the personal information may use the data for statistical analysis provided the results may not be linked to any individual or organization.

2.5.3 Cryptography Providers

Cryptography and authentication play an important role in information security. Cryptography is used to protect information in storage or in transit. Cryptography is used to transform usable information into unusable information by a process called encryption (Al-

qdah and Hui 2011). This unusable information can only be made usable by the authorized user. Information that has been encrypted can be transformed back into its original form by an authorized user who possesses the cryptographic key through a process called decryption (Information Security 2011).

The role of a service provider is to provide a service (such as the execution of an online transaction) to a customer. Digital authentication technology ensures that this service is provided to a valid customer and not an imposter (Kim *et al*. 2009). An example of a common authentication process is the use of a customer's surname in combination with a password. The use of digital signatures and biometrics are now accepted forms of authentication (Hofmeyr 2011). A critical component of digital authentication is that it has to be done in real time. A body that is responsible for local and international authentication is called the „Trust Centre'. The Trust Centre is made up of companies that provide digital authentication services. The South African Post Office, Arivia.kom and the State IT Agency (SITA) are examples of such companies in South Africa that provide digital authentication services (Seldon 2009).

A „cryptographic product' as defined by the Electronic Communications and Transactions Act of 2002 means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring the following (Kabini-Zondo 2003):

- That such data can be accessed only by relevant persons.
- The authenticity of the data.
- The integrity of the data.
- The source of the data can be correctly ascertained.

A „cryptographic service' as defined by the Act means any service which is provided to a sender or a recipient or to anyone storing a data message using cryptographic techniques for the purposes of ensuring the following (Electronic Communications and Transactions Act 2002):

- That such data or data message can be accessed or can be put into an intelligible form only by certain persons.
- That the authenticity or integrity of such data or data messages is capable of being ascertained.

- The integrity of the data or data message.
- That the source of the data or data message can be correctly ascertained.

A cryptographic provider will therefore mean any person who provides or who proposes to provide cryptographic services or products in the Republic.

The Act makes it possible for the Director-General of Communications to establish and maintain a registry of cryptography providers. The task of a cryptography provider is to use technology to provide security in the hardware and software and to maintain and monitor the security of a system (Seldon 2009).

2.5.4 Protection of Critical Databases

"Critical data" as defined by the Act means data which is declared important to the protection of the national security of the Republic or the economic and social well-being of its citizens (Electronic Communications and Transactions Act 2002).

A „critical database' as defined by the Act means a collection of critical data in electronic form where it may be accessed, reproduced or extracted (Hofmeyr 2011).

According to the Act, the Minister may declare certain classes of data as „critical' so as to protect its citizens (Electronic Communications and Transactions Act 2002).

2.5.5 Management of critical databases

The Minister of Communications has the power to formulate minimum standards regarding the following (Hofmeyr 2011):

- General management of critical databases.
- Access and control of critical databases.
- Rules regarding the security, integrity and authenticity of critical databases.
- Methods to be employed for storing of data.
- Disaster recovery plans during loss of data.

2.5.6 Cyber Inspectors

South Africa, the European Union and the United States of America have authorities that are responsible for ensuring that critical data is adequately managed. In South Africa, the Minister of Communications can appoint cyber inspectors to manage critical data. When

compared to the United States and the European Union, cyber inspectors in South Africa have a more clearer and defined role in monitoring the activities of cryptographic and authentication providers.

The role of cyber inspectors in South Africa are as follows (Cassim 2009):

- Monitor any website for any unlawful activities.
- Investigate the activities of cryptographic service providers. This will be with regard to compliance or non-compliance with the Act. The definition of a cryptographic service provider and an example of such a service provider is given in section 2.5.3.
- To order cryptographic service providers to comply with the Act if they are not complying.
- Investigate the activities of authentication service providers in relation to compliance or non-compliance with the Act. The definition of an authentication service provider and examples of such service providers are given in section 2.5.3.
- To order authentication service providers to comply with the Act if they are not complying.
- Give evidence or information to the South African police during any investigation of a cyber crime.
- Inspect, search and confiscate any information or data that may be suspicious in connection with any offence.
- Obtain a warrant of arrest from a magistrate or judge to carry out a search or inspection on those suspected of committing a cyber crime.

The European Union has Data Protection Authorities that are responsible for ensuring that critical data is adequately managed. The Data Protection Authorities are independent bodies that are responsible for enforcing national (European Union) and local (Member Country) laws (Buttarelli 2010). Each member country must set up a supervisory authority that will monitor the data protection of that particular country (Data Protection Directive 2011). Customers and business enterprises can lodge any complaints regarding personal information security to the local supervisory authority. The local supervisory authority will hear claims regarding personal information violations and this authority will be obliged to inform the persons concerned about the outcome of the claim (Buttarelli 2010).

In the United States, the Department of Justice is responsible for prosecuting cybercrimes. Under the Identity Theft and Assumption Deterrence Act of 1988, the Federal Trade Commission has the power to monitor and prosecute any unlawful activities (Jamieson *et al*. 2008). This includes the investigations of cryptographic and authentication service providers. Besides carrying out its own monitoring and investigations, the Federal Trade Commission also receives and processes all complaints from customers and business regarding the violations of personal information (Identity Theft and Identity Fraud 2011). The Commission will then refer the complaints to appropriate bodies that are responsible for handling various types of violations. The Postal Inspection Service is for example responsible for handling issues relating to theft of postal addresses. The Social Security Administration handles issues relating to the theft of a person's social security number and the Internal Revenue Service will process complaints regarding the improper use of an individual's personal information for tax violations. The United States has three principal reporting agencies that receive complaints about the theft of bank account details and credit card information. These agencies are Equifax, Experian and Trans Union. The main role of these agencies is to provide information and advice to victims when their bank and credit card information has been stolen (Identity Theft and Identity Fraud 2011).

2.5.7 Cyber Crime

Cybercrimes are crimes that are committed on the Internet (Manos 2011). One such example is the theft of a customer's personal information on the Internet. It is important that customers are educated about what constitutes a cybercrime because they will be in a position to report such crimes to the National Regulator when it occurs. Reporting a cybercrime will result in a reduction in identity theft and data breaches (Romanosky *et al*. 2008). The most crucial element of the Act is that for the first time, a person can be found guilty and convicted of cybercrime (Cassim 2009).

The interception of a customer's personal data without permission is the most common form of a cybercrime (Aaron 2010). The Monitoring Prohibition Act of 1992 protects individuals in this regard. Individuals are also protected against unauthorized interception by the South African Constitution. Section 14 of the Bill of Rights in the South African Constitution of 1996 states that "everyone has a right to privacy which includes the right not to have their communications infringed" (Privacy and Human Rights 2003: Overview 2003). The Regulation of Communications and Provision of Communication-Related Information Act

(RICA) of 2003 however is a legislation that gives certain bodies (such as a law enforcement organization) the right to intercept data without permission under certain circumstances. This legislation is in conflict with section 14 of the South African Bill of Rights of 1996. Parliament has however attempted to balance this constitutional conflict by allowing the interception of information only when serious crimes are involved (Regulation of Communications and Provision of Communication-Related Information Act 2010).

Besides interception, a cybercrime is also committed when a perpetrator (ECT ACT 2002):

- Modifies data so that it becomes ineffective.
- Sells or designs security software which is used for data interception.
- Designs or possesses any device that is used to overcome security measures.
- Commits any act that results in denial of use of a system.
- Commits computer-related extortion, fraud and forgery.

2.5.8 Penalties

The Act provides for a fine or imprisonment for those found guilty of committing computer related crimes (Cassim 2009).

2.6 The Consumer Protection Act of 2008

This legislation focuses mainly on the role of the supplier. Consumers should be aware about the legislative boundaries within which the supplier can operate. If customers suspect that business has committed any violations regarding their personal information security, then they should report such transgressions to the National Regulator.

2.6.1 The aim of the Act

The Consumer Protection Act of 2008 aims to promote a fair, accessible and sustainable marketplace for consumer products and services. Provision is also made for consumer rights and privacy (Hofmeyr 2011).

2.6.2 The provisions regarding consumer rights and privacy are as follows (Consumer Protection Act 2008).

- A supplier must only request for information that is adequate enough for the purpose of a sale or transaction. No additional information should be requested and stored.

- The supplier must have the written permission of the consumer to capture, store and distribute any information that is required.
- The consumer must have full knowledge of what information is collated, processed and stored. There is no obligation by the consumer to provide the information.
- The agreement to collect, process and store information will be valid until the expiry date.
- The supplier may not use or report any personal information after the expiry date.
- The supplier must destroy all information concerning a consumer a year after the permission has expired.
- The supplier must maintain a registry of consumers from which the information was requested.
- It becomes unlawful for any person to access information about a consumer without permission.
- When permission is granted, the person who requested for the information must keep the information confidential.

Clearly the rights of the consumer with regards to privacy and disclosure of information is protected. Consumers have recourse to the National Consumer Commission if their rights have been violated (The Protection of Personal Information Bill 2009). This body was formed after the Consumer Protection Act was passed in parliament in 2008. This body will aid in protecting consumers by investigating complaints by the consumer. The main function of this body is to issue compliance notices to suppliers and refer matters to the Tribunal or alternative dispute resolution forums. The Commission also has the power to refer any matter to the National Prosecuting Authority (Consumer Protection Act 2008).

2.7 The Protection of Personal Information Bill of 2009

When this Bill becomes an Act of Parliament this year, it will be the latest legislation regarding personal information security and will also become the most important legislation for consumers. This Bill has additional principles not contained in the Electronic Communications and Transactions Act of 2002 and The Consumer Protection Act of 2008 (Protection of Personal Information Bill 2009). The broad principles of the Protection of Personal Information Bill of 2009 are based on the principles of data protection legislation of the European Parliament known as the 95/46/EC directive.

2.7.1 Terms used in this section

This section provides an analysis of The Protection of Personal Information Bill of 2009. A comparison is also made between this legislation and similar legislation in the European Union and the United States of America. In this section, the term "data subject" means the person to whom the information relates. The data subject is generally a consumer or an individual. The term "data collector" or "responsible person" will generally refer to an individual or organization (such as an enterprise) that requests the information or already has the information.

2.7.2 The aims of the Protection of Personal Information Bill are as follows: (Protection of Personal Information Bill 2009).

- Give effect to the constitutional right to privacy by safeguarding personal information. This however, does not mean that all information regarding a consumer should be kept confidential. The law gives credence to the fact that there must be a balance between confidentiality and the right to access to information.
- Regulate the manner in which personal information may be processed. This must be done in accordance with international standards.
- Provide individuals with the rights to protect their personal information. This means that there must be legal remedies if a data collector requests and processes information beyond what is required.
- Provide remedial measures when violations have occurred. This could mean recourse to a consumer forum such as The National Consumer Commission (Protection of Personal Information Bill 2009). This body can then decide on how a resolution should take place. This could either be mediation or in some cases, the National Prosecuting Authority may become involved.

2.7.3 Conditions of lawful processing of personal information by business

The Protection of Personal Information Bill of 2009 has a section that focuses on the boundaries within which business should operate. This section is an extension of the principles contained in the Consumer Protection Act of 2008. Legislation regarding these boundaries is similar in both South Africa and the European Union (The Protection of Personal Information Bill 2009). Businesses in South Africa and the European Union

therefore have common principles which must be adhered to. The principles are as follows (Data Protection Directive 2011):

- Information must be processed lawfully and should be done in a reasonable manner so that a consumer's rights are not infringed.
- The processing should be adequate and not excessive. This means that the processing should be done for the intended purpose only. Any additional processing could lead to the infringement of a consumer's personal information.
- The consumer must agree to the processing of the data.
- The consumer must be party to the conclusion of a contract during processing of the data subject's personal information.
- The processing must be legal.
- Processing a consumer's information should be beneficial to the consumer. Processing should not lead to the violation of the consumer's personal information.
- Processing is necessary for the benefit of the consumer as well as the state or some third party.
- Based on a reasonable ground, the consumer will have the right to object to processing of his or her personal information.
- If the consumer objects then the data collector must respect the consumer's decision.

2.7.4 Purpose specification

The 95/46/EC directive and the Protection of Personal Information Bill of 2009 state that information collected should be for a specific and well defined purpose only. This purpose should also be legal. It is important that the consumer is made aware that his personal information is being collected for a specific purpose only (The Protection of Personal Information Bill 2009).

2.7.5 Retention of records

This section deals with the procedure to be adopted by business regarding the retention of an individual's personal information after the conclusion of a transaction. The Protection of Personal Information Bill of 2009 is more specific with regards to the retention of records when compared to legislation in the United States and the European Union (Data Protection Directive 2011). The Protection of Personal Information Bill of South Africa states that once personal information has been collected and the specific task achieved, the information

should not be unnecessarily retained in the database. The information can however be retained in the database for a period of one year (Hofmeyr 2011). There are however, exceptions to this. In the following instances, it may be necessary to retain personal information (The Protection of Personal Information Bill 2009):

- When stored personal information may be required by the authorities, such as the Prosecuting Authorities.
- When the consumer requests that the information should be retained.
- If information is required for statistical analysis, historical and research purposes. In such cases, safeguard mechanisms should be put in place so that the information is safe.
- If a third party uses the data with the permission of the data subject.

When a decision is taken to delete a consumer's record, it must be done in such a manner that it becomes impossible to reconstruct the information (The Protection of Personal Information Bill 2009). Legislation in the United States and the European Union does not have specific sections regarding the retention of records of customers (Data Protection Directive 2011). This means that businesses in the United States of America and the European Union can retain the personal information of customers as long as proper safeguards are in place to protect the data.

2.7.6 Further processing limitations

It may be necessary to use data collected on a customer to do further processing. This means that the customer data can be used not only for the original intended purpose, but also for other purposes not originally stipulated. Permission must however be given by the data subject before further processing can take place (Hofmeyr 2011). This can be done when the following has been taken into account (The Protection of Personal Information Bill of 2009):

- The purpose for further processing must be related to the original intention.
- The nature of the information concerned.
- The consequence to the data subject once further processing has taken place.
- The contractual rights between data collector and data subject.

Further processing can take place when (Hofmeyr 2011):

- The data subject agrees to it.

- The data becomes available in the public domain.
- It is required by the prosecuting authority such as the South African Police Services or a court of law.
- The health of the data subject or the health of the public is threatened.
- The data is required for historical, statistical analysis and research purposes.

2.7.7 Information quality and openness

The EU and South African legislation on information quality and openness is similar (The Protection of Personal Information Bill 2009). In both regions, the data collector must ensure that the information collected is complete, accurate, not misleading and should be updated at all times. This ensures the quality of the information collected.

With regard to openness, the data collector must always ensure the following during the data collection phase (Data Protection Directive 2011):

- The data subject is aware that information about him or her is being collected.
- The name and address of the subject is recorded.
- The purpose for which data is required.
- That the data subject be made aware that the data required is either mandatory or voluntary.
- The data subject needs to be made aware of the consequences if the data is not provided.
- The data subject needs to be made aware if a law or prosecuting authority requires the information.

2.7.8 Security Safeguards

One of the main challenges facing business is to ensure that personal information collected from customers is secure (Jamieson *et al*. 2008). Customers lose faith in organizations that have poor security systems that can be easily breached. The image of the company also suffers as a result of breaches (Ranger 2007). It is therefore important that organizations invest in systems that will convince customers that their personal information is secure in the hands of business. The Protection of Personal Information Bill of 2009 as well as the 95/46/EC directive of the European Union makes it mandatory for the data collector (such as a business organization) to be responsible for the security of personal information of

customers (Data Protection Directive 2011). The organization responsible for collecting the data must ensure the following (The Protection of Personal Information Bill 2009):

- That any technical or legal measure be taken to ensure that the data collected is secure.
- That unlawful access to the information is prevented.
- Identify any foreseeable risks that may occur.
- Regularly verify that safeguards are in place.
- Processing of the information is legal and has the consent of the data subject.
- If a third party has illegally attained information about the data subject, then the data subject and the Regulator must be immediately informed. The prosecuting authority may also be notified of this.

2.7.9 Data subject participation

Legislation makes it possible for a customer to exercise certain rights when their personal information is suspected of being compromised (Hofmeyr 2011). It is therefore important that customers are aware about what their rights are when an infringement of their personal information has taken place. Legally, the data subject has a right to do the following when a violation is suspected to have occurred (The Protection of Personal Information Bill 2009):

- Ask the suspect to confirm what information he or she has about the data subject.
- Provide information about third parties that may also have information about the data subject.
- Request the responsible party to pay the fee that is accrued during the investigation.
- Request the responsible party to delete any data that is inaccurate, excessive, out of date, incomplete or misleading.

2.7.10 Processing special personal information

The Protection of Personal Information Bill of 2009 makes it possible for the data collector not to process certain categories of data. The 95/46/EC directive of the European Union also has a section that specifies what categories of an individual's information should not be processed (Data Protection Directive 2011). The Protection of Personal Information Bill of 2009 is however more specific with regard to this. The responsible party may not process information in the following instance (The Protection of Personal Information Bill 2009):

- A child who is subject to parental control in terms of the law.
- A data subject in terms of his religious beliefs, political opinion, race, health, sexual life or criminal behaviour.

2.7.11 Rights of data subjects regarding Spam and automated decision making

This section focuses on legislation regarding unsolicited emails (Spam). The problems relating to Spam have prompted some countries and regions to have specific legislations that address this problem (Sund 2007). The Protection of Personal Information Bill of 2009 and the 95/46/EC directive of the European Union make provision for the following:

1. **Unsolicited electronic communications**

Legislation regarding unsolicited emails (Spam) is more stringent in the European Union when compared to the United States of America and South Africa (Privacy and Human Rights 2003: Overview 2003). The United States of America lacks uniformity in this regard as different states have their own legislation regarding unsolicited emails whereas the 95/46/EC directive of the European Union has a more uniform policy regarding Spam (Data Protection Directive 2011). Although Spam in general is not illegal in South Africa, there are certain instances when an organization can be found guilty of infringements in this regard. The Protection of Personal Information Bill of 2009 (South African Legislation) states that the processing of personal information of a data subject for the purpose of direct marketing by means of automated calling machines, facsimile machines, SMSs or e-mails is prohibited unless the following has been adhered to (The Protection of Personal Information Bill of 2009):

- The data subject has given his or her consent.
- The data subject is a customer of the responsible party. If consent is given with regard to direct marketing, the following must be adhered to:
    1) The details of the identity of the sender must be known.
    2) The address or other contact details to which the data subject can make contact with.

2. **Directories**

Many public and private organizations are creating electronic directories that contain information about individuals. The purpose is to easily provide information to individuals or

organizations that require it. If the data subject's information is put in a directory which may be in electronic format or otherwise, then he or she must be informed regarding the following (The Protection of Personal Information Bill 2009):

- The purpose of the directory.
- About any further use of the directory especially if the directory is in electronic form that contains embedded search functions.

The Protection of Personal Information Bill of 2009 explicitly states that the data subject must be given an opportunity to object if he or she does not want the personal information to be contained in the directory. He or she must also be allowed to change or update any information if the data subject chooses to leave the information in the directory.

3. Automated decision making

Automated decision making is done when functions within the system are used to create a profile of a data subject. Creating a profile is not illegal provided it does not contain aspects relating to the data subject's personality or personal habits. Profiles can however be used in the conclusion or executions of contracts (The Protection of Personal Information Bill 2009).

2.7.12 Transfer of information across borders

Since communication via the Internet has become a global phenomenon, transferring personal information across borders for the conclusion of a transaction is becoming common (Ecommerce critical components 2008). The security of the data subject's information must also be protected during the transfer of data across borders. The 95/46/EC directive of the European Union and The Protection of Personal Information Bill of 2009 (South African Legislation) make provision for the transfer of data across borders (The Protection of Personal Information Bill 2009). The information regarding a data subject may not be transferred across the border unless (Jamieson *et al*. 2008):

- The data subject agrees to it.
- The data protection principle from the requesting country is similar to our country.
- The transfer is necessary for the conclusion of a transaction and the data is then transferred with the consent of the data subject.
- It is beneficial to the data subject and the data subject gives consent for the transfer of his or her information.

2.7.13 Duties of a Regulator

South African legislation makes it possible for a National Regulator to be appointed by the Minister of Telecommunications to ensure that data is adequately managed (The Protection of Personal Information Bill 2009). In the European Union, data is managed by Data Protection Authorities while in the United States of America the Federal Trade Commission is responsible for management of the data (Identity Theft and Identity Fraud 2011). The duties of the National Regulator, the Data Protection Authorities and the Federal Trade Commission are similar. The Protection of Personal Information Bill of 2009 (this Bill is expected to become a South African law in 2011) has however explicitly defined the role of the National Regulator. The main duties of the Regulator as contained in The Protection of Personal Information Bill are as follows (The Protection of Personal Information Bill 2009):

- Promote and educate the public about their rights concerning personal data.
- To undertake research into and monitor developments in information technology related to the security of personal information.
- To monitor and enforce compliance of the Act.
- To report to parliament from time to time regarding issues relating to data protection.
- To receive and investigate complaints by the public.
- To attempt to mediate and reconcile issues between parties.
- To issue Codes of Conduct.
- To publish reports relating to protection of private and personal information.

The most important aspect of the Act is that any individual who is guilty of violating this Act may be fined or imprisoned (Cassim 2009).

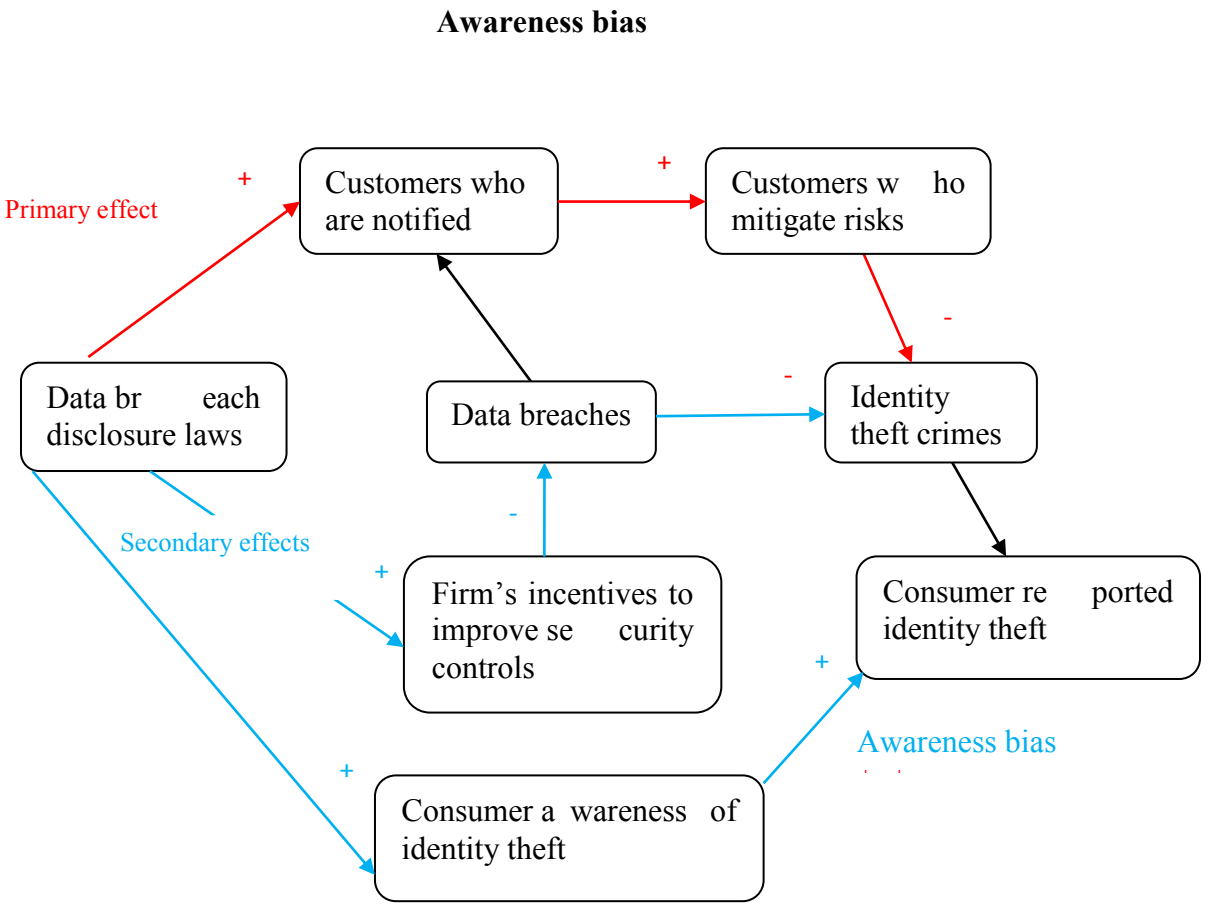
2.8 Awareness as a strategy to reduce identity crime

An extension to the conceptual model in section 2.2 (figure 2-1) is the awareness model depicted in figure 2-2 below (Romanosky *et al*. 2008). Figures 2-1 and 2-2 were formulated after empirical research was carried out on 773 breaches of US organizations collected by Attrition.org. The original conceptual model (figure 2-1) shows that as customers are notified of data breaches they will check their statements regularly. Customers will then report any irregularities to their respective business institutions. These institutions will then take steps to minimize the problem. This will result in a reduction in identity theft.

The extended awareness model (see figure 2-2 below) proposes that new consumer protection legislation will spark media attention. The media will generally have articles in magazines and newspapers educating customers about the new legislation and the steps to be taken when violations take place. An increase in media attention will result in more victims coming forward to report identity theft crimes. According to Romanosky *et al* (2008), the role of the media is as follows:

- To educate customers about their rights when violations have taken place.
- To increase customer awareness. An increase in awareness will lead to an increase in reporting of any violations.

The effect is a decrease in crimes as indicted in figure 2-3.



Source: Romanosky, Telang and Acquisti (2008)

Figure 2-2: Awareness bias

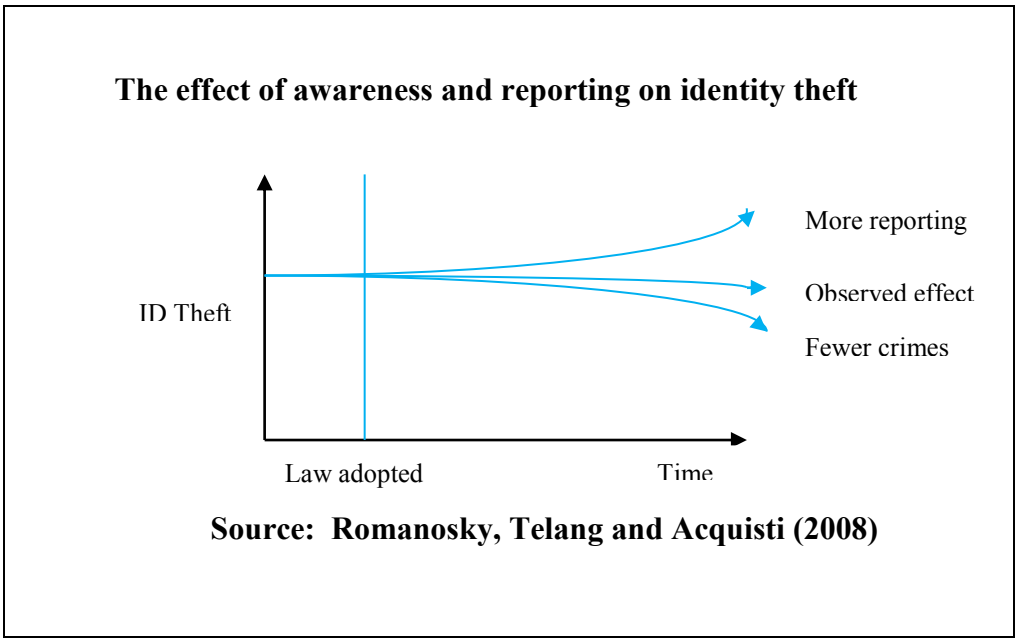


Figure 2-3: The effect of awareness and reporting on identity theft

2.9 Education as a strategy to reduce identity theft

This section discusses how Internet identity theft is perpetrated and how educating the customer will help reduce these types of crimes. Phishing as an example of Internet identity theft is discussed in this section.

Research has shown that education will not only reduce identity theft but also encourage the customer to accept new technology (Srivastava 2010). Education is therefore an important strategy that should be adopted by the government and private sector in order to reduce identity theft crimes (Jamieson *et al*. 2008). This is proposed in the framework in section 3.5.3.

Today, phishing is the most common form of identity theft (Aaron 2010). Phishing results in identity theft and financial fraud when the fraudster tricks the online users into giving their confidential information like passwords, identity numbers, credit card number and personal information such as birthdates and maiden names. The fraudster will then use the information to impersonate the victim to transfer funds from the victim's account or use the victims' information to make purchases (Nwaocha 2010). The United States of America has legislation called the Anti-Phishing Act of 2004 which aims to protect users against this crime (Laws that protect the internet from phishing, Congress and Phishing 2004). Since South Africa does not have specific legislation regarding phishing, it therefore becomes crucially important that customers are educated about how they can protect themselves against these attacks (The Protection of Personal Information Bill 2009).

2.9.1 Phishing attacks

This section provides important information on how perpetrators carry out phishing attacks. By understanding the modus operandi of perpetrators, customers can avoid becoming victims of these types of attacks (How To Avoid Getting Hooked By Phishing 2004).

Customers who bank online will normally receive legitimate emails from their banking institutions. Customers should however become wary of illegitimate emails sent by fraudsters. A customer should not respond to an email which states that (Srivastava 2007):

- You need to update your account.
- You have money due to you which you have to claim.
- There is a problem in your account and that you should provide information to correct the error.
- Your account will be closed if you do not respond to a particular email.

Responding to these emails requires that you disclose your bank account details and by doing so, you most likely will become another victim of a phishing attack. A programme regarding phishing scams that uses such methods was aired in the popular TV programmes Carte Blanche on 23 January 2011 (Christoforou and Comrie 2011). The attackers created fake banking websites that look like the legitimate ones. Customers who interacted with these websites realized that they have been scammed when they checked their financial statements. Victims of such a scam were advised to immediately contact their financial institutions to minimize the losses. The presenter of the programme also advised customers never to reveal their bank account information, credit card numbers or PIN number by email. Customers should realize that legitimate companies will not allow customers to reveal such information by email (Srivastava 2007).

Customers can also become victims when they interact with a fraudulent website that looks exactly like the legitimate one. Customers may be tempted to make a purchase by clicking on the link that allows them to order an item. When customers interact with the fake website, they disclose credit card information to this website from where it can be easily accessed by the perpetrator. The perpetrator will then use the credit card information to make fraudulent purchases (Gibbs 2011). To avoid becoming a victim of this particular type of scam, it is suggested that the customer type the URL of the department store to check whether it is legitimate or not.

Customers may notice that some of the emails they receive look suspicious. It is advisable that these suspicious emails be forwarded to companies that are being imitated. By doing so, the company will make other customers aware of these phishing emails so that appropriate action can be taken by potential victims. One such intervention is that customers will be instructed not to open these emails as the security of their personal information can be compromised (Srivastava 2007). Large companies generally have experts trained to investigate phishing scams (Brody, Mulig & Kimball 2007). Standard Bank (South Africa) is one such example of an institution that has employed experts to investigate phishing scams (Operating infrastructure 2009). Reporting phishing scams will allow the experts to investigate such cases and hopefully apprehend the perpetrators. Some financial institutions have automated mailboxes where customers can send suspicious emails to. One such example is the automated mailbox of Standard Bank which is phishing@standardbank.co.za (Christoforou and Comrie 2011). These phishing emails in the automated mailboxes will be used by the experts (who may be employed as full-time staff at the financial institution) in the field of information security and the South African Police Services to carry out investigations. It can also be used as evidence in a court of law during the litigation process.

The advice from most financial institutions is that victims of a phishing attack should contact their bank immediately to minimize the problem. Most victims who watched the programme on phishing scams on Carte Blanche (aired on 23 January 2011) responded by immediately contacting their financial institutions. These institutions immediately put a stop to any suspicious payments (Christoforou and Comrie 2011).

Another common scam which is similar to phishing involves emails indicating that the user has won a lottery and he or she is tricked into revealing information like bank account details. Dodgy investment scams will promise the user instant wealth. The user is then tricked into providing sensitive information (like bank details) to the conman or make deposits into the scammers account (Scamwatch 2011). An example of such a scam is the "Nigerian 419" scam. It is called the Nigerian scam because that is where the scam originated. The "419" is a section in Nigerian legislation that outlaws such practices (Longe *et al*. 2009). These scams are successful because payments by victims are made through Western Union. Western Union transfers are virtually untraceable and scammers are therefore using this institution for their illegal operations (Scamwatch 2011). Victims are reluctant to report these scams because they feel that they themselves have participated in an illegal activity. They do not see themselves as a victim but rather as an accessory to this type of crime (Srivastava

2007). Victims have also been threatened by the scammers if these crimes are reported to a law enforcement agency (Tanfa 2006). The individual should realize that there are no "get-rich-quick" schemes. The following signs will help online users avoid becoming a victim of the "419"scam (Scamwatch 2011):

- The scammer will request that the online user (potential victim) should help someone to transfer money out of a country. The country in question is usually one that is experiencing political instability or some conflict (e.g. Ivory Coast or Sudan).
- The scammer will usually provide a sad story as to why he or she cannot do the transfer. The common story is that he or she is trying to be protected from a corrupt government who wants to steal their wealth.
- The online user (potential victim) is promised a large sum of money in return for carrying out the request of the scammer. For the request to be carried out, the victim is forced to provide his or her banking details.
- The email is polite but is usually in broken English.

The user must therefore become wary of these scams and not reveal their personal information by email or make any payments to these phishing schemes (Srivastava 2007).

2.10 Other factors that contribute to an increase in identity theft

Legislation, awareness and education are strategies that have been employed by governments and the private sector in addressing problems relating to identity theft (Romanosky *et al*. 2008). Despite these strategies, there are many factors that contribute to identity theft not being reduced significantly.

The number of people using the Internet for commercial and personal activities has increased in the last 5 years. Consequently, there has been an increase in identity theft (Srivastava 2010). The customers themselves are partly to blame for an increase in identity theft. Customers unwittingly part with their personal information when filling out questionnaires or when a caller requests some personal information (Identity Theft Expert 2009). This is confirmed by studies carried out by Sophos, an IT based company that specializes in information security (Identity Theft Expert 2009). The study by Sophos is discussed in section 1.3.

An increase in identity theft should result in organizations upgrading their existing security measures but this is not happening. Organizations are reluctant to invest in updated security technology because of the costs involved in upgrading existing systems. Small businesses in particular are more vulnerable to attacks because they cannot afford to invest in proper security measures. Criminals know this and they will therefore target small businesses (Firewalls 2011).

The relative ease with which a perpetrator can make a purchase fraudulently also contributes to an increase in cybercrimes. Enterprises do not take the extra effort in verifying whether an individual is using somebody else's personal information to make illegal purchases (Akinsuyi 2005). An enterprise will simply turn down a customer who attempts to make an illegal purchase instead of getting a law enforcement agency to apprehend the perpetrator. Enterprises generally adopt this attitude because they feel that legislation is either inadequate or ineffective in prosecuting an offender (Manos 2011). In the United Kingdom, there is no offence for identity theft. Criminals are aware of this and will therefore continue to try different methods knowing that they are technically not committing a criminal offence (Akinsuyi 2005).

Customers and business have a role to play in reducing identity theft. Customers should become wary of scammers and not unwittingly part with their personal information. Business should make the effort in verifying that a purchase is made to a valid customer and not an imposter.

2.11 Difficulties associated with prosecuting perpetrators of cybercrimes

The very nature of the Internet with massive amounts of information being shared and the protection of personal information not being enforced has made it difficult to apprehend and prosecute cyber criminals (Manos 2011).

Changing the IP address after a cybercrime has been committed makes it difficult to identify the perpetrator. An IP address stands for "Internet Protocol" address. It is a unique address which allows one computer to communicate with another via the Internet. IP addresses allow for the pinpointing of billions of computers and devices around the world. However, detecting from where a crime originated is difficult if the IP address is changed after the cybercrime has been committed (What is an IP Address? 2011). Even if it is possible to track down the computer from where the crime was committed, it is difficult to pinpoint exactly

who committed the crime because many people (like family members) may have access to the computer. The crime may have been committed from a public place like a library that has computers available to the community. In such a case, it is virtually impossible to track down which person is responsible for committing the cybercrime (Why is cyber crime hard to prosecute? 2009). Criminals are also finding new and sophisticated methods in penetrating security measures like firewalls without leaving any "footprints". These "footprints" are the evidence that will track down and prosecute the perpetrator. Without evidence, prosecution is impossible (Firewalls 2011).

Prosecuting a perpetrator may be difficult and costly when two countries are involved. A perpetrator may operate from one country and his victims may reside in another. If there is no cooperation between the two countries concerned, then prosecuting the perpetrator becomes difficult, if not impossible (Multipoint Strategy to Fight Cybercrime 2010). The difficulty in prosecuting a perpetrator is further compounded if there are no extradition agreements between the two countries concerned. The International Criminal Police Organization (Interpol) can however only assist in apprehending a cyber criminal who resides in any one of the 186 member countries that is under its jurisdiction (Jamieson *et al*. 2008).

There are no adequate legislations to prosecute organizations (such as a business enterprise) that are negligent in protecting the personal information of customers. The Protection of Personal Information Bill of 2009 simply states that the data collector (such as a business enterprise) is responsible for the safeguarding of a customer's personal information. No mention is made of the penalty an enterprise should receive if found negligent in this regard (Protection of Personal Information Bill 2009). Investigators are also restricted by certain legislations that allow them to intercept the communications of alleged cyber criminals in certain circumstances only. The Regulation of Communications and Provision of Communication-Related Information Act (RICA) of 2003 is one such legislation that allows interception only when the crime is of a serious nature. This legislation however does not make it clear whether identity theft can be classified as a serious crime (The Regulation of Communications and Provision of Communication-Related Information Act 2010).

In order to address these difficulties, it is hoped that improvements in technology will help pinpoint and apprehend perpetrators of cybercrimes. Loopholes in present legislations should also be addressed if the prosecution rate is to be increased so that identity theft is reduced significantly.

2.12 Successful prosecutions

Despite the difficulty in apprehending cybercriminals, there are many successful prosecutions (in other parts of the world) one should take note of. The researcher decided to provide a few examples of such prosecutions. The reason for providing these examples is to show that similar prosecutions are possible in South Africa when the Protection of Personal Information Bill of 2009 becomes an Act of parliament in 2011. Since this new legislation has been formulated using legislations in the United States of America and the European Union, similar prosecutions are possible. These success stories provide greater impetus that legislation does have a role to play in addressing issues relating to cybercrime prosecutions in South Africa. The following are some examples of successful indictments in various parts of the world:

- Derek Lloyd Sykes, a British national was arrested and prosecuted in South Africa after stealing the identity of another individual in 1989 and was living under his name. The imposter was living under the name of Robert James Grant. Derek Lloyd Sykes was arrested after a passport in the name of Robert James Grant was found in his possession (Howard 2011).
- A Topeka man was indicted for crimes relating to false tax claims. Karundo Mukundi was indicted for using tax preparation software to submit false claims. He used the personal information of victims in the software to submit the false claims (Prosecutors say Kansas man facing federal tax charges tried to flee overseas 2011).
- In the Southern district of Florida, a woman was found guilty of fraudulently obtaining the driver's license of a victim and then used the information (from the license) to withdraw thousands of dollars from the victim's account (Identity Theft and Identity Fraud 2011).
- The Russian Federal Security Services successfully prosecuted Victor Pleshchuk for breaking the encryption protection code of the Royal Bank of Scotland in 2008 and obtaining the personal banking details of clients. These personal details are information contained in debit cards. The perpetrator then used the information to create counterfeit versions of the debit cards. These cards were then used in 2100 ATM's to withdraw approximately $9m (Mann 2010).
- In a Milan court, three Google executives were found guilty of posting an online video of an autistic child being bullied. Although the video was made by other

individuals, the three executive were indicted because they found that Google was irresponsible in allowing the video to be posted on the internet (Buttarelli 2010).

According to Johnson (2005), an individual's adoption of a technology (such as online transactions) is associated with the security and privacy of their personal information. Successful prosecutions will therefore lead to customers having trust in their government's ability to address security issues relating to online transactions (AlAwadhi 2009). By publicizing successful prosecutions, customers who are presently transacting online will be will encouraged to continue. Those who have not previously transacted online will be motivated to start purchasing online (Srivastava 2010). Successful prosecutions can also save a country financially. One such example is illustrated in an article that appeared in the Guardian on 2 October 2011. The article relates to how a newly formed cybercrime unit was able to save the economy of the United Kingdom £140m in six months by successfully prosecuting perpetrators of cybercrimes. Perpetrators were prosecuted for a variety of cybercrimes that included identity theft, advance fee fraud and phishing scams (Cyber Crime unit saves UK economy £140m in six months 2011).

Legislation benefits both business and customers. Legislation will make customers more aware about what their rights are regarding their personal information protection (Romanosky *et al*. 2008). This is made possible by education and awareness drives by business and government. Legislation may lead to customers transacting with more confidence and thereby increasing e-commerce activities (The Protection of Personal Information Bill 2009). Legislation has prompted business to update their security systems. Companies realize that a secure environment is beneficial to them because they will experience fewer breaches and their image is also protected (Ranger 2007). Fewer breaches result in fewer notification and litigation matters to contend with. Fewer notifications and litigations will therefore mean a savings on the part of companies.

Although legislation, awareness and education have not significantly reduced identity theft, these strategies will nevertheless enable customers to embrace technology and thereby increase ecommerce activities (Srivastava 2010). Respondents in this study also indicated that they will be more willing to embrace technology because legislation will protect them from perpetrators of cybercrime. Respondents in this study also felt that education and awareness are important strategies in reducing identity theft. Despite the difficulties and challenges business and governments experience in addressing identity theft issues, one

should however take note of the many positive outcomes that legislation, awareness and education have provided.

2.13 Conclusion

This chapter provided details of personal information security legislation in the European Union and the United States of America. The 95/46/EU Directive and the "Safe Harbor" agreements were of particular importance. Law Enforcement by INTERPOL to combat cybercrimes was also discussed. South African legislations regarding the protection of consumers were considered. Of particular importance are the Electronic Communication and Transactions Act (ECT) of 2002, The Consumer Protection Act of 2008 and the Protection of Personal Information Bill of 2009. Other strategies like awareness and education in reducing identity theft were also focussed upon. This chapter also provided reasons as to why legislation may not necessarily reduce cybercrime. Although prosecuting cybercrimes is difficult, the chapter concludes by presenting cases of successful prosecutions in various parts of the world.

Chapter 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides a description of the research methodology used in this study. It focuses on the theoretical approach that is used to guide this research as well as the approach adopted to answer the research questions.

3.2 The Research Model

The aim of the study is to determine how legislation can address the security concerns of customers so that they (customers) can embrace technology and thereby increase online transactions. It is therefore important to investigate what factors are important in motivating customers to accept and use a technology (such as the internet for transacting online). This section therefore discusses the Technology Acceptance Model as a basis for this study. The researcher also presents a discussion as to why the UTAUT (Unified Theory of Acceptance and Use of Technology) model (the most widely used model in predicting an individual's acceptance of technology) is not used in this study. The general Technology Acceptance Model of Davis (1989) is then discussed followed by a discussion of the Extended Technology Model of Mitchell (1999). A discussion is also presented on how The Conceptual Research Model of Johnson (2005) can be used for the development of a secure information system.

3.2.1 The Technology Acceptance Model

Although the most widely used model in predicting an individual's acceptance of new technology is the UTAUT (Unified Theory of Acceptance and Use of Technology Model) model (AlAwadhi 2009), it will not form the basis of this study. The UTAUT model is formed through a review and consolidation of constructs from eight (8) models which includes the Technology Acceptance Model. The UTAUT model takes into consideration many factors such as performance expectancy, facilitating conditions, voluntariness of use, effort expectancy, social influence, gender and age. The only factor that is of importance in this study is security which is related to performance expectancy. Security, however, can be addressed using The Technology Acceptance Model. The researcher therefore decided to use the Technology Acceptance Model instead of the UTAUT model as basis for this study.

The Technology Acceptance Model suggests that when users are presented with new technologies, two important factors will influence their decision, namely (Safeena *et al*. 2011):

- Perceived usefulness and
- Perceived ease-of-use.

Perceived ease of use and perceived usefulness predict attitudes toward use of technology. Attitude toward use predicts the behavioural intention to use. Finally intention predicts the actual use of the technology (Davis 1989). If the technology is indeed useful and easy to use, then the individual will accept the technology. The converse will, however, also be true. If the technology is not useful and is difficult to use, then the user will reject the technology. A user will either accept or reject the technology. The main dependent constructs are behavioural intension to use and system usage. The main independent constructs are perceived usefulness and perceived ease of use. The Technology Acceptance Model is depicted in figure 3-1.

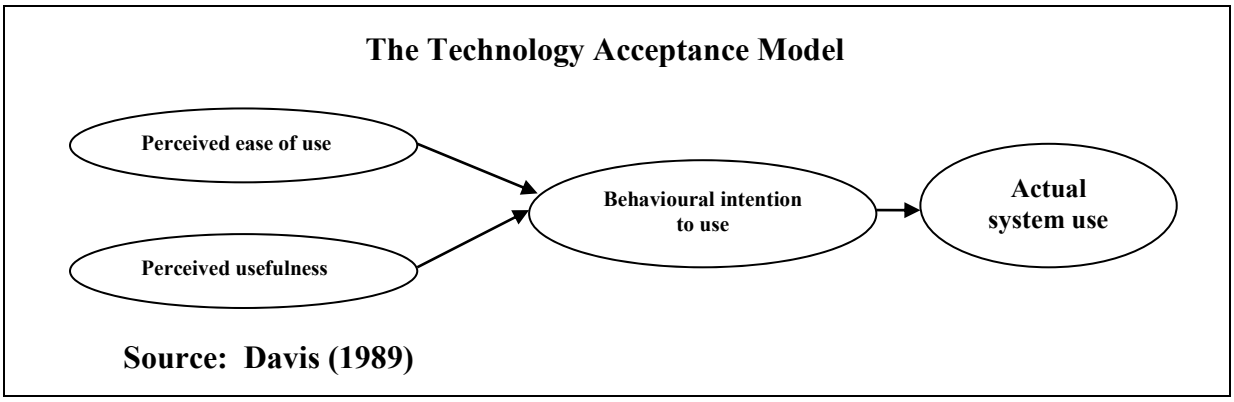


Figure 3-1: The Technology Acceptance Model

3.2.2 The Technological Acceptance Model applied to Ecommerce activities

Mitchell (1999) extends the Technology Acceptance Model by taking perceived risks into account. According to Mitchell (1999), consumers will avoid using a new technology if they feel that there are risks and uncertainties involved. An example of such a risk is crimes committed on the Internet. Internet associated risks have been integrated with the model (see figure 3-2 below). Although the technology may be easy to use and is useful, customers will reject this technology because of the perceived risks. Consumer perceptions regarding these

risks should therefore be addressed if the technology is to be embraced. Legislation, awareness and education are strategies that can be employed to address these risks.

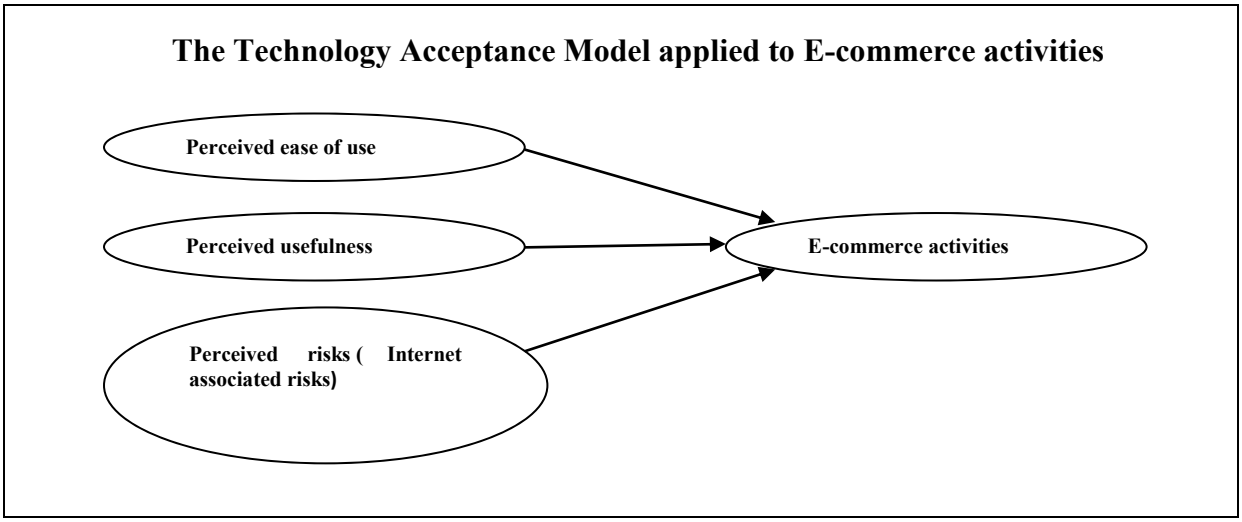


Figure 3-2: The Technology Acceptance Model applied to E-commerce activities

3.2.3 The Conceptual Research Model

Section 3.2.2 provided a discussion on the Extended Technology Model of Mitchell (1999) which posits that an individual will avoid using technology if there are perceived risks involved. This section discusses how these risks can be addressed using the Conceptual Research Model of Johnson (2005) so that customers will embrace technology and not avoid it. The Conceptual Research model is formulated using research about the Technology Acceptance Model (Davis 1989). From an organizational perspective, it proposes the study of the following as indicated in the Conceptual Research Model in figure 3-3:

- The influences of a set of external variables on perceived usefulness of information security.
- The influences of the perceived usefulness of information security on the actual investment in information security.

This study uses the Conceptual Research Model as a theoretical basis for the development of an information security model. Jamieson *et al* (2008) propose external variables such as legislation, awareness and education as the most important strategies that should be adopted to reduce identity theft. There are, however, other external variables that also have an influence on information security. All the external variables are illustrated in figure 3-3 below.

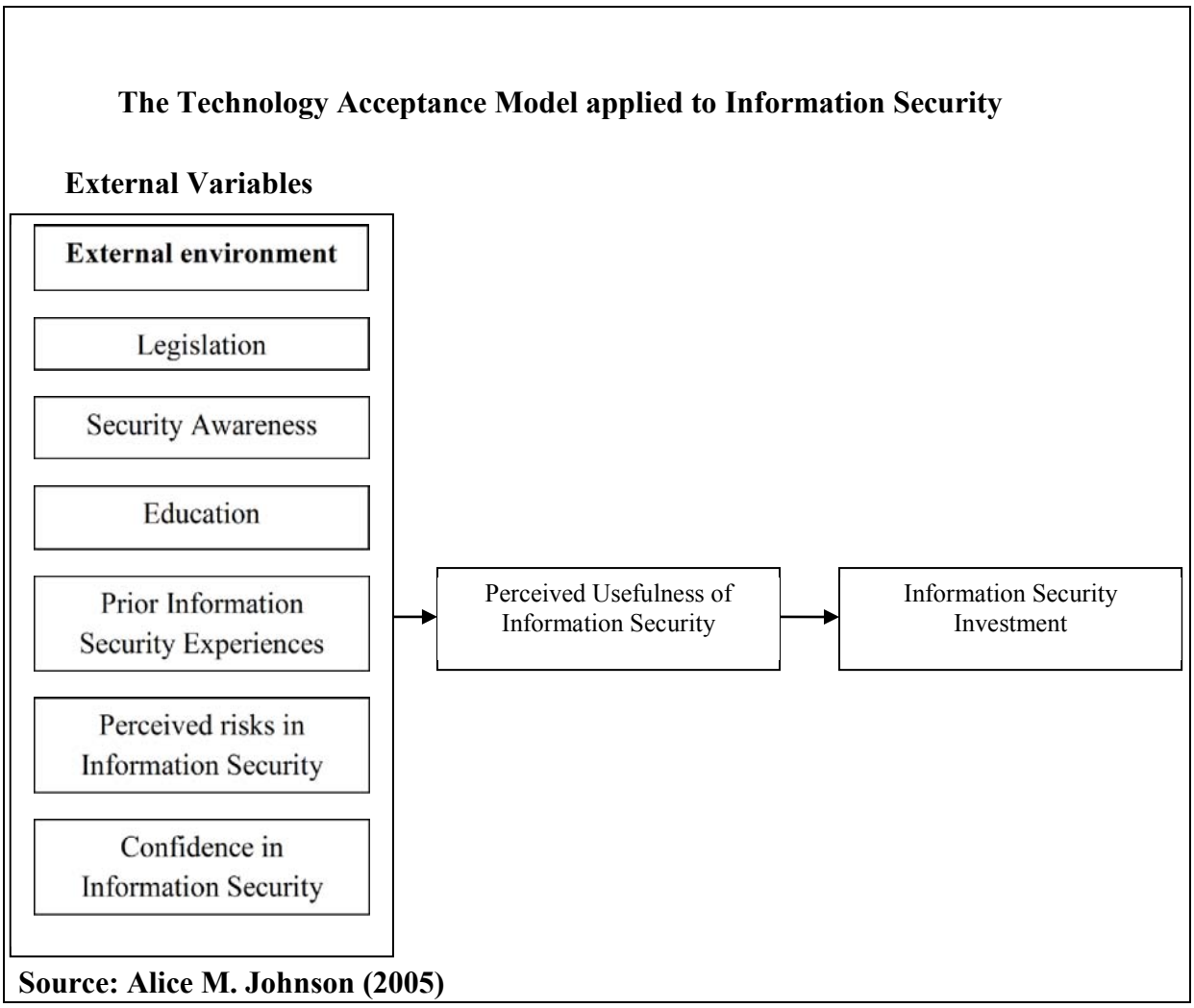


Figure 3-3: Conceptual Research model

Research has shown that business organizations benefit when there are investments in information security (Romanosky *et al*. 2008). The most important benefit of a secure information system is that the customers' confidence in transacting online will increase so that they can embrace the technology. This will result in an increase in ecommerce activities and an increase in income for companies (Srivastava 2010). The main aim of the research is therefore to determine how legislation can address the security concerns of customers so that they (customers) can embrace technology and thereby increase online transactions. The Conceptual Research Model in figure 3-3 therefore has legislation as one of the variables that addresses the security concerns of customers. Legislation is therefore considered as an investment by the state to address security issues regarding personal information. According to the Protection of Personal Information Bill (Republic of South Africa 2009), legislation will provide confidence to consumers that their personal information is safe in the hands of business. Legislation will also provide a platform for customers to take the necessary steps

when they become victims of identity theft. The Conceptual Research Model also has "confidence in information security" as one of the variables that are important to customers. Research has shown that customers have more confidence in businesses that invest in updated security systems when compared to businesses that employ outdated security measures (Firewalls 2011). Business should therefore invest in a secure environment to reduce data breaches and gain the confidence of customers. Education and awareness programmes are also variables that are included in the model as important factors in reducing identity theft (Johnson 2005). Business and government must therefore invest in awareness and education campaigns to reduce identity theft (Jamieson *et al*. 2008). Education and awareness drives will result in fewer victims of identity theft and business will experience fewer breaches (Acquisti *et al*. 2008). The framework also takes into consideration prior information security experiences, confidence in information security and perceived risks as factors that influence the development of the information security model. Customers will most likely not support enterprises that have a record of prior breaches as they will lose confidence in these organizations (Ranger 2007). Organizations that have experienced breaches in the past should therefore invest in updated security controls to win back the support and confidence of customers (Srivastava 2010).

3.2.4 The Conceptual Research Model as a guide for this study

The state and organizations need to invest in strategies to address the security concerns of customers. The most important strategies are legislation, awareness and education (Jamieson *et al*. 2008). This study and The Conceptual Research Model take these strategies into consideration. The model focuses on investments in security as an important component in developing a secure information system (Johnson 2005). Research has shown that consumers will more likely make purchases from an enterprise that has a secure information system and avoid those that experiences breaches (Ranger 2007). The Model therefore proposes that organizations should invest in information security if they are to be accepted by individuals (Johnson 2005). The use of the Conceptual Research Model is appropriate because the focus in this research is also on investment. In this study, the state and companies should invest in legislation, awareness and education. The model was successfully employed to study user acceptance of microcomputers (Igbaria *et al*. 1989) and the World Wide Web (Lederer *et al*. 2000).

3.3 Problem Statement

The Internet Security Problem has deterred customers from conducting business electronically (Castaneda *et al*. 2007). Customers fear that their personal information can be intercepted when transacting online (Online Banking Concerns 2011). Other fears include the changing of data with malicious intent, denial of use, hacking, deliberate disclosure of confidential information and e-mail associated risks (Nwaocha 2010). Identity theft or the theft of Personal Identifiable Information has also contributed to customers' reluctance in transacting online. Perpetrators can use the personal information of the customer to take over their account or use the information to make illegal applications (Fraud: awareness and prevention 2011). The government has passed legislation which aims to address the fears and concerns of customers. The Electronic Communications and Transactions Act of 2002), the Consumer Protection Act of 2008 and the Protection of Personal Information Bill of 2009 (which is expected to be passed in parliament in 2011) are such examples. Customers need to be aware about these legislations so that they can take appropriate steps if they become victims of identity fraud (Jamieson *et al*. 2008). Legislation should also make customers embrace technology with the knowledge that they are legally protected (The Protection of Personal Information Bill 2009).

3.4 Research Questions

This dissertation aims to answer the following research questions:

- How does legislation address the concerns of customers regarding their personal information security?
- What are consumers' attitudes towards their personal information security?
- How knowledgeable are customer's about consumer protection legislation?

3.5 The theoretical framework guiding this research

This section provides the theoretical background regarding security on the Internet. An identity fraud strategy is also provided which governments should adopt to protect customers.

3.5.1 Privacy as a humans rights issue

Privacy is a fundamental human right. The United Nations included it as part of its Universal Declaration of Human Rights in 1948 (Volio 1981). Privacy and consumer protection is a broad concept in our society (Margulis 1997). In this context, however, our focus is on the

Internet and the consumers need for privacy when transacting online. One of the strategies that governments should adopt to protect customers against privacy violations is legislation.

3.5.2 The dimensionality of customer privacy concern on the internet

Enterprises require information about consumers. Since the information has to be accessed, consumers are concerned about the security of the information (Castaneda *et al*. 2007). Personal information in digital form can be easily copied, transmitted and integrated into profiles (of customers) which make it easy for online marketers to construct descriptions of consumers. Websites can be accessed and unsolicited e-mail (Spam) can be sent to consumers. Despite the risks and vulnerabilities, consumers benefit because they can get personalized online service. Researchers and upper management benefit since the information can be used to determine trends. Statistical analysis can also be easily done. Organizations can also legally use the information for marketing purposes provided it (the information) does not identify who the information belongs to. Therefore to maximize e-commerce, Government has to adopt strategies to manage the personal information of customers.

3.5.3 Identity Fraud Strategy: A conceptual framework for governments

Internet identity theft has become the most common cybercrime and is costing organizations and Governments millions in prevention, control, detection and prosecution (Aaron 2010). The huge financial cost has prompted Governments to find strategies to limit identity theft. According to Jamieson *et al* (2008), Governments and organizations that are proactive and implement a strong framework have several advantages compared to those that do not. Firstly, proactive organizations generally demonstrate a willingness to curb the "insider attack", such as employees and ex-employees. Secondly, executive management of proactive organizations would take steps to measure, manage and mitigate the identity theft problem. Thirdly, suitable strategies are employed by successful Governments as indicated in figure 3-4.

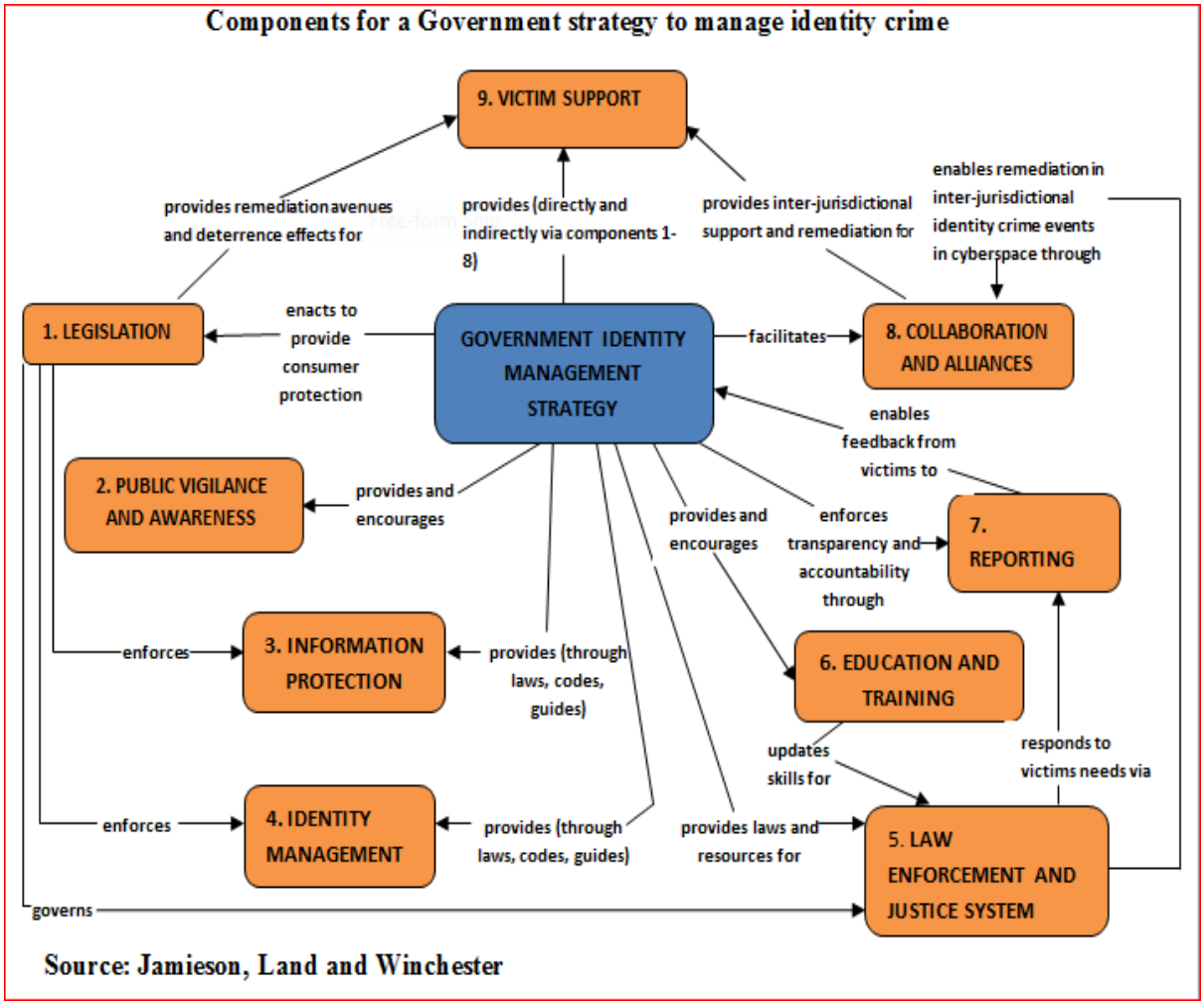


Figure 3-4: Components for a government strategy to manage identity theft

The critical components identified in the framework include legislation, public vigilance and awareness programs, information protection, identity management, law enforcement and justice systems, education and training, reporting procedures, collaboration and alliances, and victim support. These are the areas Governments and business should be focussing on in order to reduce identity theft (Romanosky *et al*. 2008).

According to the framework, legislation (component 1) enforces information protection (component 3) and identity management (component 4) through laws, codes and guides. The model proposes that public vigilance and awareness (component 2) be encouraged (Jamieson *et al*. 2008). Linked to this component is the component called reporting procedures (component 7). Increase in awareness will lead to an increase in reporting when a breach occurs (Romanosky *et al*. 2008). This will lead to an increase in media attention. Companies and individuals will desist from committing identity fraud for the fear of being exposed (Ranger 2007). The effect is that awareness will lead to more reporting and more publicity.

This will result in a reduction in crime. The law enforcement and justice systems (component 5) will prevent and reduce the incidence of identity fraud from deterrence, detection, prevention and control to remediation and recovery through the legislative process (The Protection of Personal Information Bill 2009). This component will also be responsible for victim support (component 9). Educating and training (component 6) can also help prevent and detect identity crime. This component will help consumers take preventive measures to limit identity crimes (How To Avoid Getting Hooked By Pfishing 2004). Component 8 (collaboration and alliances) relates to cooperation across borders such as the role INTERPOL will play to reduce identity fraud. All member countries will have criminal information through a variety of databases. The idea is that countries will cooperate with each other to prosecute perpetrators of identity fraud (Jamieson *et al*. 2008).

The implementation of the framework does not however guarantee that there will be a significant decrease in identity theft (Manos 2011). There are many factors that hamper the efforts of government and business. These factors are presented as a counter argument in section 2.8. The most important being the difficulty in apprehending and prosecuting a perpetrator of cybercrime (Akinsuyi 2005).

3.6 Research Design and Methodology

This section provides a description of the approach that was adopted for the collection and analyses of primary data.

3.6.1 Research methodology and the research questions

The aim of the framework in section 3.5 is to help Governments understand identity theft crimes and what steps should be taken to reduce these types of crimes (Jamieson *et al*. 2008). According to the framework, the most important strategies that governments should employ to reduce identity theft are legislation, education and awareness. This study therefore examines how legislation can address the security concerns of customers as well as their (the customers) knowledge regarding consumer protection legislation. It also investigates the attitudes of customers regarding their personal information security. We therefore need to adopt a research methodology that will answer these questions.

3.6.2 The Research Approach

According to Bryman (2004) research strategy refers to the general orientation when conducting research. This generally involves a quantitative or qualitative approach. Research design refers to a framework for the collection and analysis of data (Bryman 2004).

The purpose of the study is to answer the following research questions:

- How does legislation address the concerns of customers regarding their personal information security?
- What are consumers' attitudes towards their personal information security?
- How knowledgeable are customers' about consumer protection legislation?

A quantitative approach is adopted to answer these questions. A quantitative approach is chosen in this research because a similar study was successfully conducted in the United States of America using this approach. The study was conducted by Rhoda Marissa Clossum (2010) for her Master's thesis. The title of the study was "A Quantitative Study of Citizen Awareness, Concern and Information Seeking Behaviour Related to the Use of the Social Security Number as a Personal Identifier" (Clossum 2010). An online survey of adult university students and other community members was employed. The results indicated that awareness levels differed according to the age of the respondents.

The study conducted by Clossum (2010) adopted a quantitative approach over a qualitative approach. When the nature and scope of the study is examined, a quantitative approach was chosen because it was easier to analyse the huge volume of data collected (Clossum 2010). The quantitative approach enabled the researcher to control the investigation and the structure of the study. This would not have been possible if a qualitative approach was adopted because the qualitative approach is unstructured and this study is structured. Unlike unstructured surveys, a structured survey requires the respondent to choose one answer from many alternatives (Welman *et al*. 2009). The research design involved the use of structured questionnaires containing close-ended Likert-type scale questions. This study also adopts a quantitative approach.

3.6.3 The Questionnaire

Questionnaires are also referred to as self-completion questionnaires and are the most popular method in eliciting responses from the respondents. Open and closed questions are the two

types of questions that can be asked (Welman *et al*. 2009). Open questions require respondents to answer in their own terms. Closed questions have answers which respondents are required to choose from. For this study, close ended Likert-type questions are asked.

Bryman (2004) provides many suggestions when drawing up a questionnaire. Although all the suggestions were taken into consideration, the following three are the most important and therefore worth mentioning.

- The research questions must be kept in mind when drawing up the questions.
- The language used should be simple and precise. The language must be suitable for the target population.
- No double-barrelled questions should be asked. An example of such a question in a Likert-type scale is "Legislation and education can reduce identity theft." In this case, the respondent may agree with the first part and disagree with the second.

It is advisable that the questionnaire should not be lengthy, as fatigue may set in. The questionnaire for this study, however, is a bit lengthy because of the nature of the topic. The researcher felt comfortable with this as the respondents are academics and they (the respondents) were given at least one week to fill in the questionnaire. Most of the respondents indicated that they did not fill in the questionnaire in one sitting. They indicated that they completed the questionnaire in at least two sittings.

3.6.4 Testing the questionnaire

The target population for the study are the staff at Durban University of Technology. The questionnaire was therefore tested with five academics at this institution. They were chosen on the following basis:

- A staff member who is actively involved in online shopping.
- A member who has never made any purchases online and is not motivated to do so in the future.
- A member who is a victim of identity theft.
- A Lecturer in Information Systems who provided valuable input regarding the content of the questionnaire.
- A Lecturer in Communications who assisted with issues relating to the suitability of the language used.

The objective of this exercise was to test the following:

- How long it will take to answer the questions. The researcher averaged the time to answer the questions to be twenty five minutes.
- Whether the language used is suitable. The respondents felt that the language was not difficult to comprehend. The Lecturer in Communications was most helpful in correcting the grammatical errors.
- How relevant the questions are regarding the objectives and the research questions. In this case the respondents felt that the questions were in line with the objectives and research questions. The Lecturer in Information Systems provided valuable input on the section regarding customers' attitudes towards their personal information security.

3.6.5 The Layout of the Questionnaire

This section focuses on how the questionnaire was devised. A discussion on research constructs is first provided. A table which indicates how these constructs are linked to the research model is then presented. An explanation of each section of the questionnaire then follows.

Constructs describe the unobservable (such as attitude) which is articulated by the respondent during the data gathering process of the study. Constructs are also referred to as latent variables. On the other hand, measures are defined as observed scores that are gathered through an interview, self-report, observation or some other means. Measures are quantifiable and are gathered from a survey instrument such as a Likert scale (Hardin *et al*. 2010).

Measures (also called indicators) can be influenced by latent variables. These are known as reflective constructs. Reflective constructs will assume that the latent construct will cause the variations in the measures. For example, the Perceived Ease of Use Model of Davis (1989) is measured by six reflective indicators: easy to learn, controllable, clear and understandable, flexible, easy to become skilful, and easy to use. An increase in Perceived Ease of Use will be reflected by an increase in all six indicators. This means that all measures in a reflective model are expected to be correlated. The high correlation between indicators means that all indicators are interchangeable and dropping an indicator will not alter the meaning of the construct (Petter *et al*. 2007).

A formative construct on the other hand can influence latent variables. The indicators of a formative construct are not highly correlated and therefore these measures are not interchangeable. Unlike reflective constructs, all indicators of a formative construct may not have to move in a certain direction simultaneously (i.e. increase or decrease). An example of a formative construct is that an increase or decrease in identity theft is directly related to legislation, education and awareness (Jamieson *et al*. 2008). An increase in awareness will for example decrease identity theft (Romanosky *et al*. 2008) even though there may not be an increase in legislation (an increase in legislation will mean an improvement of present legislations or the introduction of new legislations) or education.

The main aim of the research is to determine how legislation can address the security concerns of customers so that they (customers) can embrace technology and thereby increase online transactions. Table 3-1 below indicates what research construct (reflective or formative) is used for each section of the questionnaire in order to achieve the main goal of the study.

Section	Question Number	Research Construct
A	Background Information	-
B	6,7	These questions relate to credit card usage as well as online shopping. The key variables from the Conceptual Research Model in figure 3-3 relating to these questions are prior information security experiences and perceived risks in Information Security. Respondents may not have had any prior negative experiences (such as online fraud) therefore they will embrace the technology and shop online. On the other hand, respondents may have had a negative experience (such as a data breach) and therefore they will not embrace technology (Ranger 2007). Their decision to transact online will also depend on their perceptions on perceived risks in Information Security (Castaneda *et al*. 2007). These perceptions may also be negative or positive. Since there is a high correlation between both variables (prior information security experiences and perceived risks) reflective construct is more appropriate.
C	1 to 14	This section relate to customers' attitudes toward their personal information security. The appropriate variables for these questions from the model in figure 3-3 are perceived risks in Information Security and Confidence in Information Security. According to Mitchell (1999), individuals will avoid a

		technology if there are perceived risks associated with the technology. Customers also need to feel confident that their personal information is safe in the hands of business. They will therefore avoid organizations that experience breaches (Ranger 2007). Since there is a high correlation between both variables (perceived risks in Information Security and Confidence in Information Security) reflective construct is more appropriate.
D	1 to 7	This section relates to consumers' opinions regarding the use of strategies such as legislation, awareness and education to address the Internet Security Problem. Since there may not be a high correlation between indicators, formative construct is more appropriate for these questions.
E	1 to 5	This section tests the respondents about their knowledge on The Electronic Communications and Transactions Act of 2002. The important variables from the model in figure 3-3 are legislation, awareness and education. Since knowledge and awareness is being tested, there may not be a high correlation between indicators therefore formative construct is more appropriate.
F	1 to 7	This section deals with the boundaries within which a business can operate as contained in The Consumer Protection Act of 2008. The important variables from the model are legislation, awareness and education. Since knowledge and awareness is being tested, there may not be a high correlation between indicators therefore formative construct is more appropriate.
G	1 to 12	These questions focus on the rights of a consumer when personal information is requested by an enterprise. The important variables from the model are legislation, awareness and education. Since knowledge and awareness is being tested, there may not be a high correlation between indicators therefore formative construct is more appropriate.

Table 3-1: Research Constructs

It is important for a questionnaire to have background information as well as clearly defined objectives. The questionnaire should also have guidelines on how to answer the questions. The background, objectives and guidelines are contained in section A.

General questions (such as age and gender) and specific questions (such as credit and shopping card application, online shopping, etc) are first asked. Bryman (2004) suggests that

these types of questions are important to put the answers into context. These contextual type questions are asked in section B of the questionnaire.

The questions on consumer attitudes are asked in section C of the questionnaire. The objective of these questions is to determine what consumers' attitudes are regarding their personal information protection. This section contains 14 questions. The three legislations (The Electronic Communications and Transactions Act of 2002, The Consumer Protection Act of 2008 and The Protection of Personal Information Bill of 2009) on personal information security were studied and relevant questions were drawn up for the questionnaire. For each of the questions, respondents used a five-point Likert scale to rate their attitude from "Strongly Agree" to "Strongly Disagree".

Section D contains seven questions. The objective of these questions is to elicit the opinions of customers on issues relating to Legislation, Awareness, Education and Security Issues. It is important to find out from customers themselves whether strategies such as Legislation, Education and Awareness will reduce identity theft. A five-point Likert scale is used to rate the opinions of the consumer. This ranges from "Strongly Agree" to "Strongly Disagree".

One of the objectives of the study is to determine how knowledgeable consumers are on specific legislation relating to their personal information protection. Section E tests the respondents about their knowledge on The Electronic Communications and Transactions Act of 2002. This is an important piece of legislation because for the first time it becomes possible to prosecute a perpetrator for cybercrime. The researcher formulated five questions for this section. A five-point Likert scale is used to rate the customers knowledge from "Am fully aware of this" to "Am totally unaware of this".

Section F contains questions that will test the consumer's knowledge on The Consumer Protection Act of 2008. This section contains seven questions. Here, the role of the supplier is focussed upon. These questions will make the consumer aware about the legislative boundaries within which the supplier can operate. A five-point Likert scale is used to rate the respondents knowledge from "Am fully aware of this" to "Am totally unaware of this".

Section G tests the respondents' knowledge on the Protection of Personal Information Bill of 2009. This will be the latest legislation (when this Bill becomes law in 2011) regarding personal information security and is also the most important for consumers. The researcher chose twelve of the most important questions from this Bill. These questions focus on the

rights of a consumer when personal information is requested by an enterprise. It is important that consumers become knowledgeable about what their rights are when surrendering their personal information to a company. This section contains twelve questions. A five point rating scale ranging from "Am totally aware of this" to "Am totally unaware of this" is used.

3.6.6 Population

Bryman (2004) defines a population as the universe of units from which the sample is to be selected. The term unit is used because it is not necessarily people that are being sampled. The researcher may want to sample from a population of cities, organizations, schools, etc. The population in this study is the staff at Durban University of Technology. Lecturers from the five faculties as well as personnel from the Department of Information Communications and Technology make up the population.

The main aim of the study is to determine how legislation can address the security concerns of customers so that they (customers) can embrace technology and thereby increase online transactions. In order to achieve the main aim of the study, respondents should be computer literate and have access to the internet in order to be suitable for the study. All staff members (i.e. the population) have access to the internet and the selected sample will therefore be useful in the study. The results of the study can also be generalised to the broader university population because they are computer literate and they have access to internet and email.

3.6.7 Sampling

Welman *et al* (2009) define sampling as a segment of a population that is to be investigated. A sample is a representative of a larger group. By studying a sample, we learn the characteristic of the population (Thompson 1999). It is easier and cheaper to study a sample rather than study an entire population. Analysing the data of a sample is also quicker and more accurate as compared to an entire population. However, in this study the researcher attempted to get responses from all personnel from the various faculties (i.e. the census).

A sample can be selected on a probability or non-probability basis. In probability sampling, each sample unit has a known non-zero probability of being selected. The most common type of probability sampling is the simple random sample. In non-probability sampling, the probability of selection is not known. The selection of units is arbitrary. The most common type of non-probability sampling is convenience sampling (Welman *et al*. 2009). Bryman (2004) describes convenience sampling as one that is simply available to the researcher. The

researcher would not have to spend time looking for the participants. For this study, the researcher has used convenience sampling to select the participants.

When the research questions of this study are examined, the respondent's gender, age, race and academic status are not considered because these factors may play a minimum role in this study. The only criteria in selecting the respondents' is that they should be computer literate and they should be able to execute routine tasks such as email. All members of staff at Durban University of Technology have access to technology such as computers and the Internet and they are therefore suitable as respondents for this study. It is for these reasons that non-probability sampling is chosen as method for selecting the participants. The researcher is a staff member at Durban University of Technology and choosing convenience sampling provides an added advantage since the participants of the study are available to the researcher.

Research on individuals' attitudes and awareness regarding personal information security was successfully conducted using convenience sampling and a quantitative approach. An example of such a study was carried out in Ireland (Lang *et al*. 2009). The aim of the study was to report on findings regarding university students' attitudes and awareness of the risks associated when interacting with social networking sites. Convenience sampling was used to select respondents from one of the main universities in Ireland. The findings indicated that students adopted a very casual attitude towards password protection which could compromise their personal information security. Most of the students were not aware of threats posed by viruses and illegal interception (Lang *et al*. 2009). This study and the research carried out in Ireland is similar, therefore the researcher decided to use convenience sampling when selecting the respondents.

3.6.8 Distribution of the Questionnaire

The researcher felt that it would be appropriate to distribute the questionnaire online using Google documents. Online distribution makes data capturing and processing easier (Wright 2005). Online distribution was tried at the satellite campus in Pietermaritzburg. The response rate was unfortunately very low and the researcher therefore decided to abandon this method of data collection. Only two (2) respondents from a staff complement of seventy four (74) completed the questionnaire online. The researcher therefore decided to make hardcopies of the questionnaire for the respondent to fill in manually.

The questionnaires were hand delivered to each Faculty. The researcher made an appointment with each of the Deans in the five faculties. They were very cooperative and agreed to assist in the data collection process. Two Deans agreed to personally assist in the entire process, from distribution to collection of the questionnaires. Three Deans assigned the task to a staff member in their faculty to coordinate the entire process. The researcher suggested to the Deans that the questionnaire be given to all staff members in their respective faculties. The researcher gave them one week to complete the process.

A total of four hundred and twenty (470) questionnaires were distributed. One hundred and eight (108) questionnaires were completed and returned. Seven (7) questionnaires were either incomplete or incorrectly filled. The data from the seven (7) spoilt copies could therefore not be used in the investigation. The data of the remaining one hundred and one (101) questionnaires are used in the study.

The breakdown of the returns is as follows:

Faculty/Department	Number of returns
1) Engineering	23
2) Arts	15
3) Economic and Management Sc.	9
4) Accounting and Informatics	30
5) Health Sciences	6
6) ICT	18

Table 3-2: Breakdown of returns

3.6.9 Data Analysis

The data collected from the responses are analysed with the Statistical Package for Social Sciences (SPSS) version 18.0 as well as Microsoft Excel. SPSS has facilities for the extensive manipulation and transformation of data. Fully labelled graphs and tables can also be easily done. Most researchers use SPSS because of its power and flexibility. The results for this study will be presented in the form of graphs, cross tabulations and other figures.

3.6.10 Ethical Considerations

The respondents must be assured that the information they provide will be kept confidential. An informed consent form was prepared and sent to the participants who were assured that

the information they provided will be kept confidential. It was also important to emphasise that their participation in the study is voluntary. The informed consent form contained the following information which the participants were made aware of:

- The name of the researcher;
- The name of the supervisor;
- The name of the institution supporting the research (see Annexure D);
- The objectives of the study;
- That the respondents' participation is voluntary and that he or she can withdraw from the study at any time.

Further, the questionnaire did not request for the participant's name, ID number, address or any other information that could identify the respondent. This further helped in keeping all information confidential.

A staff list for each faculty was obtained and handed to the Dean of each faculty. This helped in keeping track on who the questionnaire was given to and who returned the completed ones. This helped to ensure that the responses are valid.

3.7 Conclusion

This chapter discussed the research design and the methodology used in answering the research questions. The Technology Acceptance Model and a theoretical framework that guides the study were first discussed. The methodology used to answer the research questions was then discussed in detail. The chapter concludes with a discussion on the importance of having ethical clearance before the questionnaires are distributed.

Chapter 4

RESULTS OF THE QUANTITATIVE ANALYSIS

4.1 Introduction

The previous chapter discussed the research design and the methodology used in the study. It focussed mainly on how primary data was collected for analysis. This chapter presents the results of the research after the primary data was captured and analysed. The software that was used to do the analysis is the package called the Statistical Package for Social Sciences (SPSS) version 18.0. Most of the tables were done in MS Excel. The results will be presented in the form of graphs, cross tabulations and other figures.

4.2 Reliability and Validity

In order to determine how precise the results are, it is important to test its reliability and validity. Reliability is computed by taking several measurements on the same subjects. A reliability coefficient of 0.70 or higher is considered as "acceptable" (Refer to Annexure B for an explanation on how reliability is calculated.)

The results are presented below.

Section	Reliability
Attitude criteria regarding consumers' personal information security	0.802
Legislation, Awareness, Education and Security Issues	0.706
Electronic Communications and Transactions Act of 2002	0.888
The Consumer Protection Act of 2008	0.935
The Protection of Personal Information Bill of 2009	0.964
Overall	0.934

Table 4-1: Results of the reliability scores for the five sections in the questionnaire

Each individual section in table 4-1 produced a score of more than 0.7. The average reliability score of all the sections is 0.934. One can therefore conclude that the responses were consistent. Since the calculations for reliability yields a value of 0.7 or greater (for the individual sections and the overall average), one can also conclude that the respondents' scoring was not random.

4.3 Presentation of the results

The following changes regarding the presentation of the results are made:

- In the questionnaire (Annexure A), sections regarding credit and shopping card ownership, online shopping, consumer attitudes and consumer opinions have the following Likert scale from which the respondents can choose. These are "Strongly Agree", "Agree", "Neutral (Not Sure)", "Disagree" and "Strongly Disagree". The researcher decided to combine the categories "Strongly Agree" and "Agree" into a single option called "Agree" because these options convey the same message. Similarly, the categories "Disagree" and "Strongly Disagree" have been collapsed into one category called "Disagree" because these two options will also convey the same message. Combining these categories will also provide a more accurate analysis of the results. The graphs will now have the scales as "Agree", "Neutral" and "Disagree".
- In the questionnaire (Annexure A), sections regarding the customers' knowledge on consumer protection legislation have the following Likert scale from which the respondents can choose. These are "Am fully aware of this", "Am aware of this but more clarity is needed", "Not sure (may have read or heard about this)", "Generally unaware of this although I may or may not heard about this" and "Am totally unaware of this". In order to present a more accurate analysis of the results, the responses for the first two are combined and presented in the graphs as "Aware" and the responses for the fourth and fifth are combined and presented as "Uncertain". The responses for ""Not sure" is presented as "Uncertain".

4.4 A comparison of the sample with the population

It is important to indicate whether the sample reflects the demographics of the university. In the study, the demographics chosen are gender, academic rank, faculty and location of the campus. Table 4-3 shows a comparison of the sample with the population. The demographics chosen are represented in the first row and the first column of the table below.

Comparison Of The Sample With The Population							
Faculty	**Accounting and Informatics**	**Economic & Management Sciences**	**Engineering**	**Health Sciences**	**Arts**	**ICT**	**Total**
Total staff complement	47 (males) + 50 (females) =97	42 (males) + 56 (females) = 98	126 (males) + 29 (females) = 155	33 (males) + 52(females) =85	23 (males) + 32 (females) =55	18 (males) + 14 (female) =32	289(males) 233 (females) = 55% (males) and 45 % (females)
Total responses collected	30	9	23	6	15	18	101
Percentage	31%	9%	15%	7%	27%	56%	20%
Number of Staff based in Durban	76	86	124	85	45	32	448
Response collected from Durban	25	3	22	6	10	18	84
Percentage	33%	3%	18%	7%	22%	56%	18.75%
Number of staff based in Pietermaritzburg	21	12	31	Nil	10	Nil	74
Responses from Pietermaritzburg	5	6	1	Nil	5	Nil	17
Percentage	24%	50%	3%	Nil	50%	Nil	23%
Number of male respondents in both campuses	14	6	18	2	7	11	58
Percentage	14.5%	6%	12%	2%	13%	34%	11%
Number of female respondents in both campuses	16	3	5	4	8	7	43
Percentage	16.5%	3%	5%	5%	14%	22%	8%

Table 4-2: Demographics at DUT

The above table gives us some demographics about the Durban University of Technology. There are a total of 522 permanent staff members who are either academics or who belong to the ICT department. A total of 448 staff members are based in Durban and 74 are based in Pietermaritzburg. This is the target group in our investigation. Personnel from the Information Communications and Technology (ICT) departments were included in the study because they are in the Information Technology field and their input would therefore be useful. It is expected that staff from the ICT department would be more knowledgeable about issues relating to personal information security. Temporary teaching personnel, secretaries, technicians, maintenance workers, security personnel and staff from the library and Human Resources departments are not included in the study.

A total of 101 completed responses were received. This means that approximately 20% of respondents completed the questionnaires. Eighty three (83) responses were received from Durban and 18 were received from Pietermaritzburg. This means that there were 18.5% of

respondents from Durban and 24% from Pietermaritzburg. The ICT department had by far the highest proportion (56%) followed by the Faculty of Accounting and Informatics (31%) and Arts (27%). The least number of responses were received from the Faculty of Economic and Management Sciences (9%) and Health Science (7%). Engineering (15%) has a fairly significant proportion of responses. When all faculties and departments are compared, ICT had the most number of male respondents (34%) while Economic and Management Sciences had the least number of female respondents (3%). In total, 58% of respondents were males and 42% were females.

Although some interesting demographics are presented, it is important to point out that some of the information that was requested could not be provided by the human resource department at Durban University of Technology. There was no information available on the age of each personnel from the population. Although the age of the respondent is obtained from the questionnaire, it could not be compared with the age of the population (since the Human Resource Department could not provide this information).

4.5 Results of the investigation and the research questions

It is important that the results answer the research questions. The research questions are as follows:

1) How does legislation address the concerns of customers regarding their personal information security?
2) What are consumers' attitudes towards their personal information security?
3) How knowledgeable are customers' about consumer protection legislation?

4.6 Statistical terms used in this chapter

This section provides a brief description of terms that are used in this chapter regarding the analysis and presentation of results.

4.6.1 Descriptive Statistics

Descriptive statistics describes the organising and summarising of quantitative data. Descriptive statistics are useful as it summarises results for an experiment, thereby also allowing for more constructive research after more detailed analysis. Descriptive data analysis aims to describe the data and the distribution of scores on each variable (Johnson and Bhattacharyya 2006).

4.6.2 Cross-tabulations

A cross-tabulation is a description of data resulting from observations made on two different related categorical variables. This is usually presented in a summarised form using a table, known as a two way frequency table or contingency table (Johnson and Bhattacharyya 2006).

4.6.3 Frequency

Given a collection of data values, the specification of all the distinct values in the collection together with the number of times each of these values occurs in the collection is called the frequency distribution. The number of times a value occurs is called the frequency (*f*).

4.7 Frequency with respect to gender, age and status

This section provides a brief description of the respondents in terms of their gender, age and status.

4.7.1 Frequency for males and females

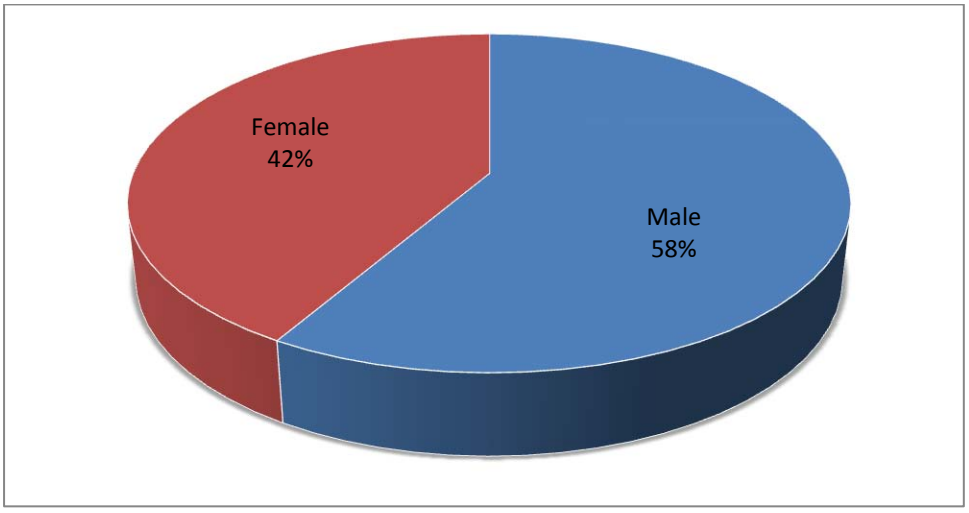


Figure 4-1: Description in terms of gender

The number of male respondents (58%) compares closely with the total number of males in the population (55%) as indicated in table 4-2. Female respondents (42%) also compared favourably with the number of females in the population (45%) as indicated in table 4-2.

4.7.2 Frequency in terms of age

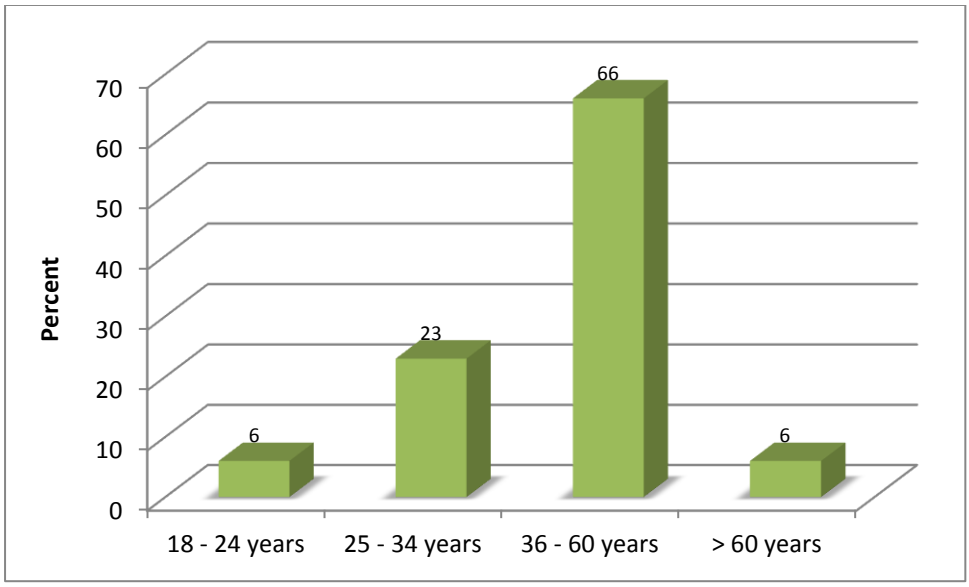


Figure 4-2: Description in terms of age

Nearly two thirds (66%) of the respondents were between the ages of 36 and 60 years.

4.7.3 Description in terms of academic status

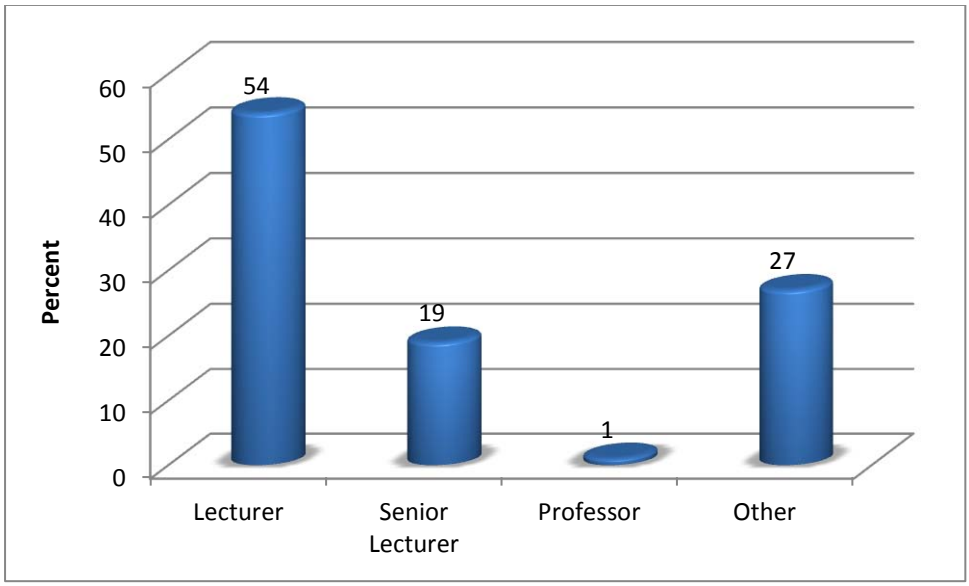


Figure 4-3: Description in terms of status

More than half of the respondents (54%) were lecturers. Academic staff comprised nearly three quarters (73%) of the sample. The rest of the respondents (27%) comprised non -

academic staff. This group is made up of personnel from the Information Communications and Technology (ICT) department.

Research question 1

The results of the Chi-square test will be interpreted to answer the first research question.

Pearson Chi-Square Tests	Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
	New legislation has been passed to address customer security concerns and therefore customers should not be afraid to transact online.	According to legislation, monitoring and recording a user's browsing habits is illegal.	According to legislation, Spam is illegal	Research has shown that security concerns have resulted in a decline in e-commerce activities	Awareness programmes leads to more reporting and hence a decline in the crime rate.	Educational programmes will protect customers against criminal activities
1. I am reluctant to disclose my personal information because of security concerns.	0.106	0.143	.000*	0.851	.000*	0.914
2. When business has collected my personal information, I want to have more control over the information. In other words, I could instruct business to modify or delete the information.	.003*	.047*	.000*	0.157	.000*	0.498
3. I am willing to disclose my personal information provided I have full knowledge of what information is collated, processed and stored.	.005*	.018*	.019*	.009*	0.187	0.492
4. I am reluctant to disclose my personal information to business because I do not have a say on how the information is being used.	.026*	.000*	.003*	.001*	0.806	0.341
5. The lack of security clauses in contracts and transactions discourages me from disclosing my personal information.	.001*	0.547	.000*	0.092	0.852	0.629
6. The introduction of new technology generally increases my concern about my personal information security. I therefore avoid disclosing my information when new technology is introduced.	.005*	0.23	.000*	.001*	0.312	0.297
7. I do not know who has access to my personal information, therefore I limit the amount of information I disclose to business.	0.051	0.056	.000*	.000*	0.351	0.322
8. I am concerned that business may use my personal information for purposes not originally intended. Nevertheless, I will disclose my information because I need to make the purchase.	.000*	.013*	.000*	0.184	0.182	0.184
9. I avoid surfing the net because I know that my navigation details are being recorded.	0.100	0.051	.018*	0.127	0.111	0.404
10. I limit or avoid shopping online because I am concerned about the security of my personal details (like bank details).	.043*	0.119	.015*	0.157	0.751	0.865
11. When personal information is required, I normally question the data collector about the security of my personal information.	0.139	.019*	.000*	0.144	.000*	0.303
12. If I question the security procedures of an enterprise, I feel I may not be allowed to make the purchase.	.000*	.000*	.002*	.010*	0.404	0.273
13. Codes of conduct refer to rules that are devised by an organization (in-house rules) that may not necessarily be contested in a court of law. Codes of conduct will encourage me to disclose my personal information.	.001*	.000*	.000*	.000*	.003*	.034*
14. New legislation (such as the Protection of Personal Information Bill of 2009) will encourage me to readily disclose my personal information to an enterprise as I feel more protected.	.000*	.000*	.000*	.000*	.039*	.000*

Table 4-3: Results of Pearson Chi-Square Tests

Government has taken consumer's concerns into account when drafting consumer protection legislation (Protection of Personal Information Bill 2009). The Electronic Communications and Transactions Act of 2002, The Consumer Protection Act of 2008 and the Protection of Personal Information Bill of 2009 have sections that specifically deal with the protection of personal information of consumers. It is therefore important to determine how significant the relationship between customers' concerns, legislation, security and education are in order to answer the first research question. Pearson Chi-Square Tests are used to determine the strength of this relationship (Refer to Annexure C on how a Pearson Chi-Square test is conducted). Values ≤ 0.05 are considered significant. Fourteen (14) questions regarding customer concerns are indicated in table 4-3. Columns 1, 2, and 3 indicate sections of legislation that address concerns relating to illegal monitoring, illegal recording and interception as well as Spam. These are the main concerns of customers (Castaneda *et al*. 2007). Column 4 deals with security, column 5 deals with awareness and column 6 deals with education. The results of the Pearson Chi-Square Test are indicated in the remainder of the cells.

The Chi Square results indicate that there are significant relationships for 58% of the cross tabulation statements regarding the security concerns of customers and legislation. This is clearly indicated for the cross tabulation value (p value of .009) of statement 3 and column 4. This cross tabulation indicates that customers will only disclose their personal information if they are convinced that it is secure. A similar conclusion can be drawn from the cross tabulations of statement 4 and column 4 (p value of .001) as well as statement 7 and column 4 (p value of .000). The Protection of Personal Information Bill of 2009 addresses the security concerns of customers by having a section which states that the data collector (such as a business enterprise) is responsible for the security of customer's information. Most of the security questions showed significant relationships with legislation as well as illegal monitoring and recording of customers' personal information. Customers are protected against illegal interception and monitoring by the Monitoring Prohibition Act of 1992. Of particular significance is that all 14 questions showed significant relationships with Spam indicating that the Chi Square conditions for Spam has been met. Customers regard Spam as an invasion of their privacy and a threat to the security of their personal information (What are the effects of Computer Hacking? 2010). Customers feel that by responding to Spam their personal information is at risk of being compromised. They are therefore reluctant to transact online as indicated in the cross tabulations for statement 1 and column 3 (p value of

.000), statement 6 and column 3 (p value of .000), statement 9 and column 3 (p value of .018), statement 10 and column 3 (p value of .015). Although Spam is not illegal in South Africa, the processing of personal information of a customer for direct marketing using Spam is illegal (Protection of Personal Information Bill 2009).

Questions 2, 3, 4, 8 and 12 relate to customers concerns' regarding the disclosure of personal information to business. These questions showed significant relationships with legislation (first 3 columns) indicating that the Chi Square conditions regarding the disclosure of personal information to business has been met. This means that customers want legislation to make it possible for them to have full knowledge of what information is collated and stored. These are indicated in the cross tabulations of statement 3 and columns 1, 2 and 3 with p values .005, .018 and .019 respectively. They also want legislation to make it possible for a customer to delete or modify any information that is incorrect as indicated by the p values .003, .047 and .000 (i.e. the cross tabulations of statement 2 with columns 1, 2 and 3). The Consumer Protection Act of 2008 makes it possible for customers to have knowledge of what information is collected by business. They also have the right to request to an enterprise to correct or remove information that is incorrect (The Consumer Protection Act 2008). Customers feel that if legislation will allow them to have a say on how their personal information is used then they will willingly disclose their personal information to business. Customers are also concerned that business will use the information they have collected for purposes not originally intended and they want legislation to protect them in this regard. This is indicated with p values .000, .013 and .000 (cross tabulation of statement 8 with columns 1, 2 and 3). Legislation has been passed which makes provision for these concerns (The Protection of Personal Information Bill 2009). Customers are, however, not knowledgeable about these legislations as indicated in figures 4-10, 4-11 and 4-12.

Nine (9) of the questions did not show any significant relationships with awareness (5^{th} column) and the first 12 questions did not show any significant relationship with education (last column). Most of the questions, however, showed significant relationship with legislation (first 3 columns). This means that customers regard legislation as more significant when compared to awareness and education.

When all 14 questions regarding consumer attitudes are examined, the last 2 proved to be most significant as all of the column variables indicated a significant relationship. This indicates that the Chi Square conditions for all 14 questions as well as all 6 columns have

been met with p values being significant (i.e. the p values are ≤ 0.05) In other words, legislation (first 3 column statements), security (4^{th} column statement) and education (5^{th} and 6^{th} column statements) have a significant impact with regard to code of conduct and new legislation (questions 13 and 14 on customer concerns). The importance of this is that when all 14 questions are examined, customers regard codes of conduct and new legislation (questions 13 and 14) as the most effective in addressing issues relating to personal information security.

Questions 1,5,7,9 and 10 had single or at most 2 significant values with respect to legislation, security and education. This means that these questions have no significant relationship with legislation, security and education because customers in this category are generally not knowledgeable about legislation and security issues as indicated in graphs 4-10, 4-11 and 4-12. The p values for these cross tabulations are > 0.05 indicating that the Chi Square conditions for questions 1, 5, 7, 9, and 10 have not been met. To attain significant values (i.e. values ≤ 0.05) in this category, customers will have to become more knowledgeable about legislation regarding their personal information protection. More knowledge results in greater acceptance of a technology (Srivastava 2010).

The aim of legislation is to provide confidence to customers that they should not be afraid to transact online because they are protected by legislation (Protection of Personal Information Bill 2009). The results show that there is a significant relationship between most of the questions on customer concerns and legislation. Awareness and education programme did not, however, show any significant relationships with reference to the 14 questions except for the last two statements regarding codes of conduct and the Protection of Personal Information Bill of 2009. The results therefore confirm that legislation is an important strategy in addressing the security concerns of consumers.

Research question 2 is answered in section 4.10 and the third research question is answered in section 4.12.

4.8 Credit Card and shopping card ownership

This section presents the results of the investigation on credit card and shopping card ownership. An analysis of the results is then done.

4.8.1 Results in terms of customers who own shopping or credit cards

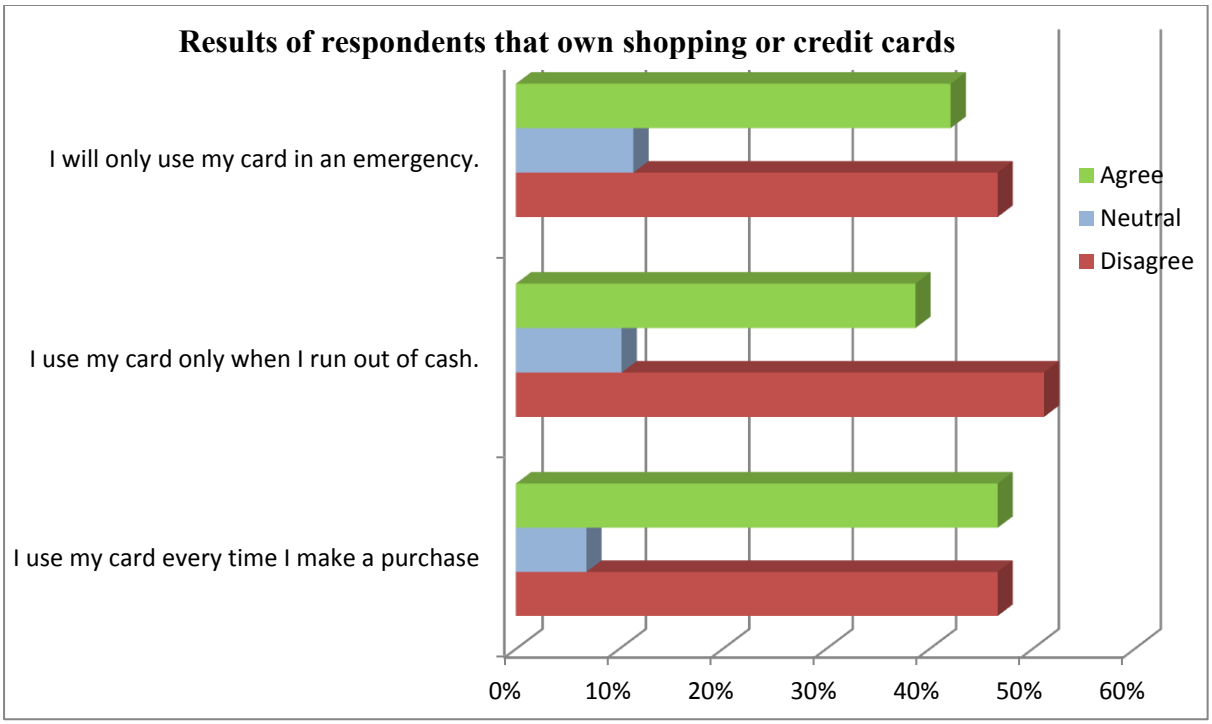


Figure 4-4: Respondents that own shopping or credit cards

The level of agreement is similar for all three questions with an average close to 40%. The level of disagreement for all three questions is also similar but with an average close to 47%. Close to 45% of respondents use their card every time they make a purchase while a similar percent will not use their card for every purchase they make. One needs to examine why less than 40% of respondents will only use their cards when they run out of cash and why only 40% of respondents will only use their cards in an emergency. This means that on average, more than half the respondents will avoid using their shopping or credit cards if possible. This low percentage of card usage is related to the Internet security issues that concerns customers. People will limit the use of shopping and credit cards because of the perceived risks involved (Online Banking Concerns 2011). This is also in keeping with the theory of Mitchell (1999). His theory states that individuals will limit their use of technology if there are risks involved.

Clearly there is a split between those that agree and those that are in disagreement for all three questions. Half of the respondents that are in disagreement are concerned about the security issues (Online Banking Concerns 2011). They are victims of identity theft or they do not have adequate knowledge of consumer protection legislation that is available for their protection. Half of the respondents that are in agreement have not been victims of identity

theft or they are knowledgeable about consumer protection legislations. Customers who are knowledgeable about personal information security will be more motivated to embrace technology when compared to those with little or no knowledge (Srivastava 2010). This group (those that are in agreement) will therefore use the technology to the fullest without being concerned about security issues because they will rely on legislation for their protection.

4.8.2 Results in terms of customers who do not own cards

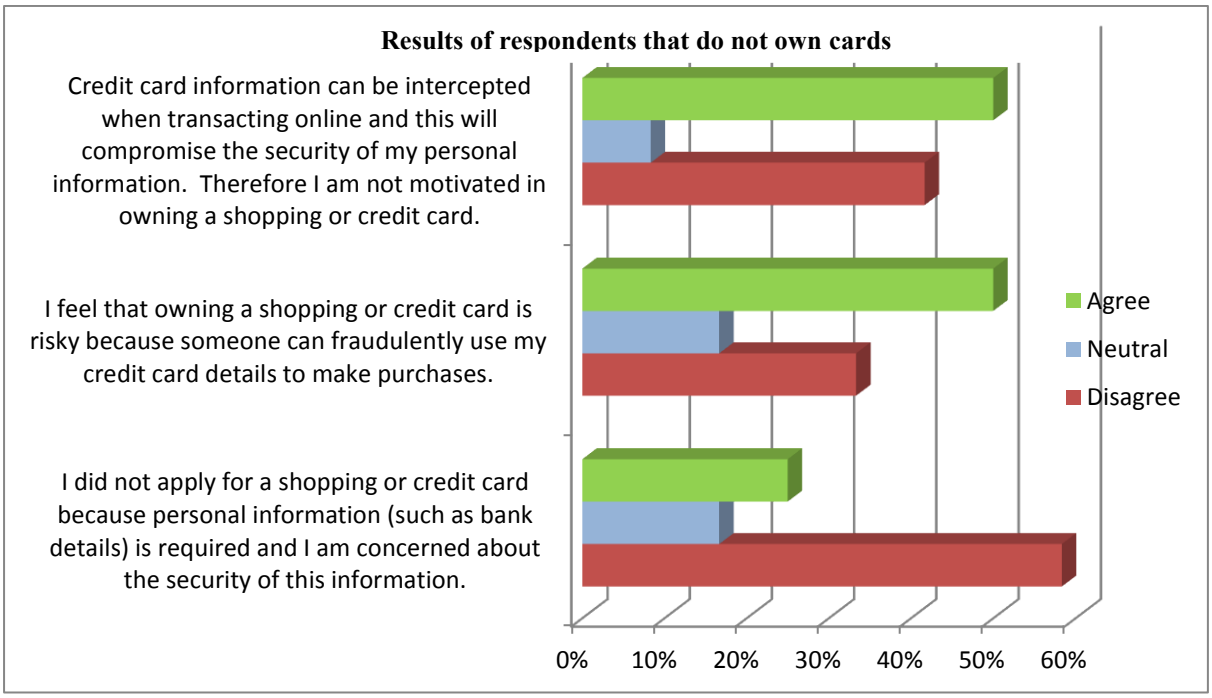


Figure 4-5: Respondents that do not own cards (such as shopping or credit cards)

An equal number (close to 50%) of respondents are in agreement with the first two questions. From the response regarding these two questions, one can conclude that most respondents are concerned that their personal information can be intercepted when they are using shopping or credit cards. They also fear that when their credit or shopping cards are stolen, perpetrators can fraudulently use their cards to make illegal purchases. This is in keeping with the theory espoused by Mitchell (1999) which states that individuals will avoid using a technology when there are risks involved.

Close to 60% disagreed that they do not own a shopping or credit card because personal information like bank details is required. This is the highest level of disagreement for all three questions. This means that respondents from this group either prefer physically going

to the store and pay cash for their purchases or they will shop online and make payments using the method of Electronic Funds Transfer (EFT). EFT does not require the use of cards.

On average, less than 20% of respondents were neutral on all three questions. This means that close to 80% of respondents are certain and decisive about the option they have chosen. Most respondents are therefore convinced that security issues deter them from owning cards (shopping or credit cards) or they will use more secure means of online payments that does not require the use of cards (such as EFTs).

4.9 Online shopping

This section focuses on the results of the investigation on online shopping. An analysis of the results is then done. Table 4-5 indicates the percentage that shop online and the percentage that do not.

4.9.1 Frequency in terms of those that shop online

Customers that shop online			Total
Do you shop online?	Yes	Count	32
		% of Total	31.7%
	No	Count	69
		% of Total	68.3%
Total		Count	101
		% of Total	100.0%

Table 4-4: Percentage that shop online

Only 32% of the respondents shop online while two thirds (68%) do not shop online.

4.9.2 Results relating to respondents who shop online

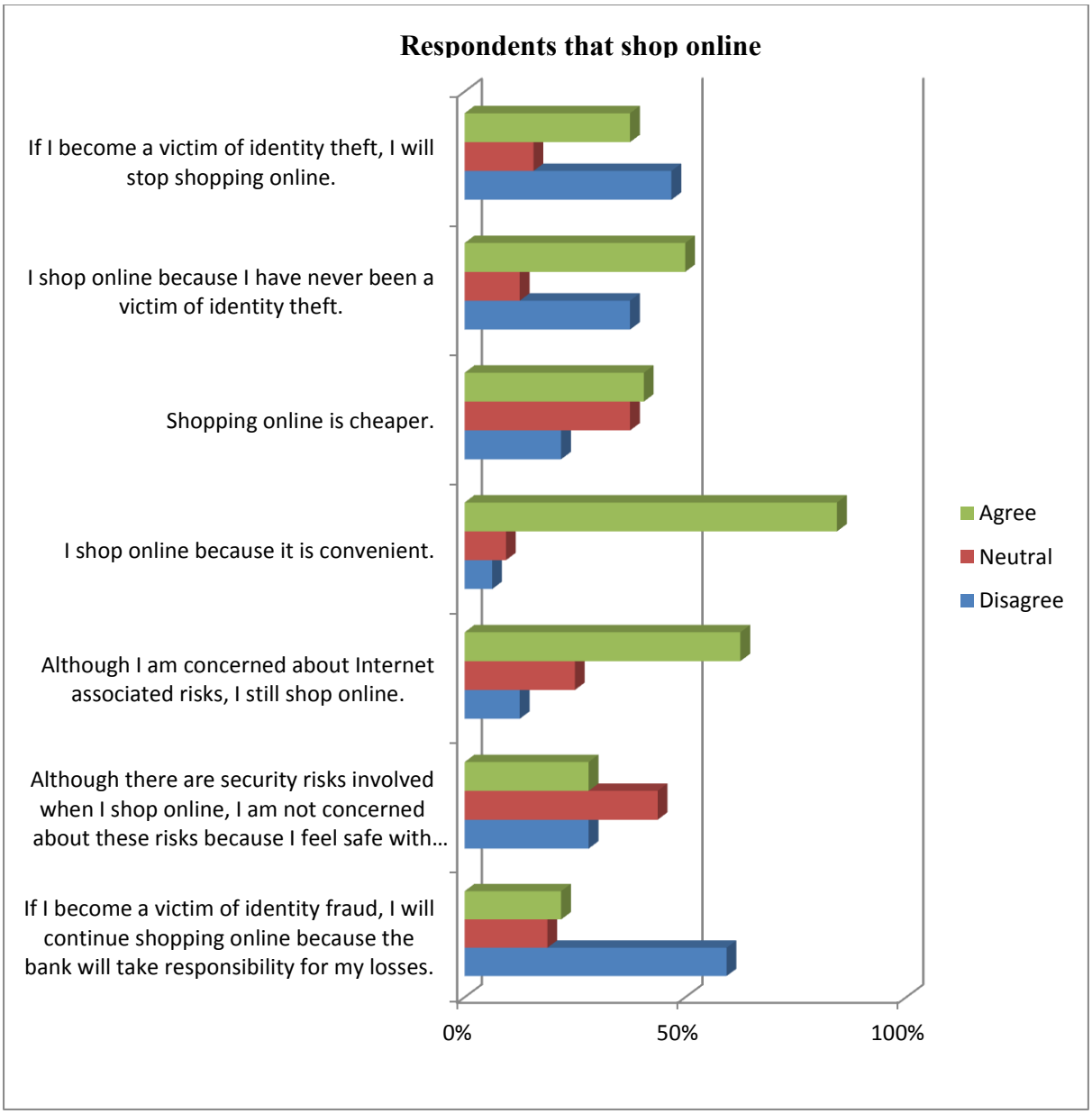


Figure 4-6: Results of respondents that shop online

Close to 30% of respondents agreed that if they became a victim of identity theft, then they will stop shopping online while 18% of respondents were neutral on this. It is interesting to note that 45% of respondents will continue shopping online even though they may become victims of identity theft. This may be related to the following statements:

- "I shop online because it is convenient" to which 80% of the respondents agreed.
- "Although I am concerned about Internet associated risks, I will still shop online" to which 60% of the respondents agreed.

Clearly, 45% of the respondents felt that the convenience of online shopping is an overriding factor for them to continue despite Internet associated risks. Customers that are actively engaged in online shopping tend to be more aware and knowledgeable about security issues when compared to those that do not (Srivastava 2010). Therefore to increase ecommerce activities, awareness campaigns and education are important strategies.

At least half the respondents (50%) shop online because they have never been a victim of identity theft. Just over than half the respondents (58%) will not continue with online shopping if they become a victim of identity fraud (even though the banks may take responsibility for victims' losses). This is in accordance with theory espoused by Mitchell (1999). Mitchell (1999) extends the Technological Acceptance Model by taking risks into account. According to his theory, consumers will avoid or discontinue using a new technology if they feel that there are risks and uncertainties involved. An example of such a risk is crimes committed on the Internet. Consumer perceptions regarding these risks should therefore be addressed if the technology is to be embraced (Mitchell 1999).

From the graphs in figures 4-10, 4-11 and 4-12, it can be observed that more than half the respondents do not understand important consumer protection legislation that concerns them. This could be the reason why only 28% of respondents agreed to the statement "Although there are security risks involved when I shop online, I am not concerned about these risks because I feel safe with new consumer protection laws." Government would want this percentage to increase as this will mean an increase in ecommerce activities. Knowledge about legislation will increase ecommerce activities as knowledge will result in greater acceptance of the technology (Srivastava 2010). This can be achieved with greater awareness and education as indicated in the conceptual framework in section 3.5.3.

4.9.3 Results of respondents that do not shop online

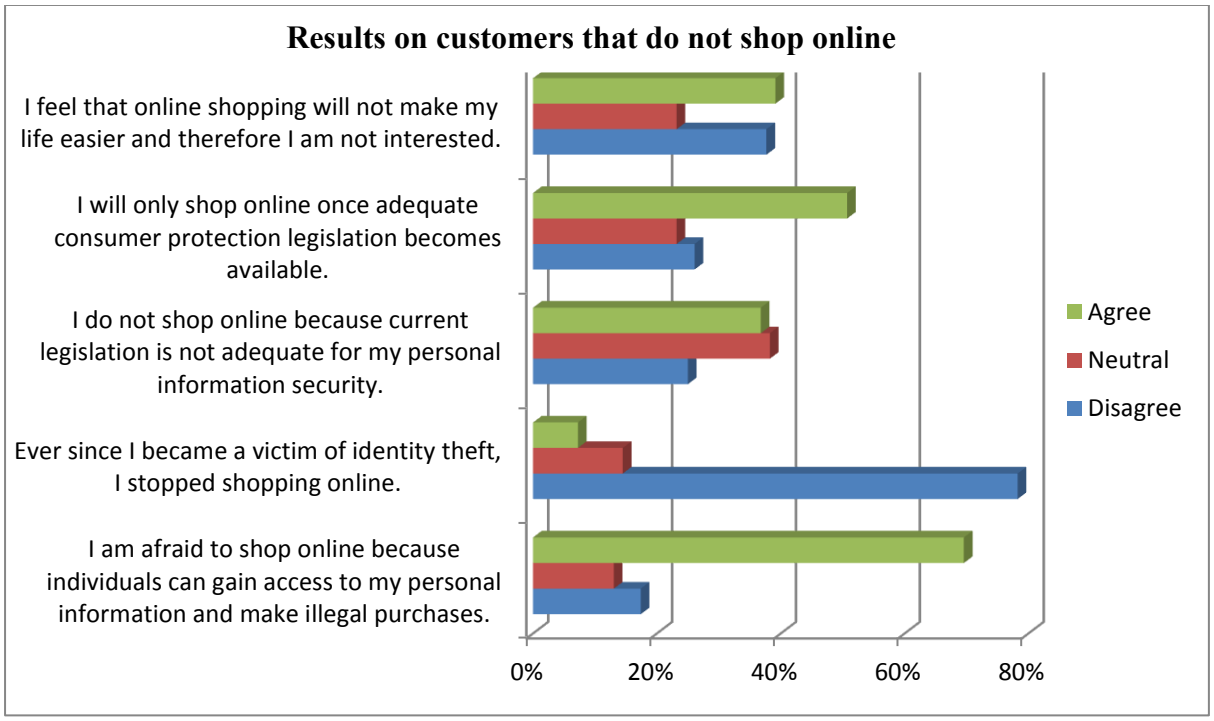


Figure 4-7: Customers that do not shop online

One of the concerns customers have relate to how secure their information is when they are transacting online (Online Banking Concerns 2011). This is confirmed with the results of the study as indicated in figure 4-7. Close to 70% of respondents are afraid to shop online because they feel that individuals can gain access to their personal information and make illegal purchases. The results also indicate that close to 50% of the respondents will choose to shop online once adequate consumer protection legislation becomes available (see question 2 of figure 4-7). There are however, adequate legislation available which respondents are unaware of as indicated in figures 4-10, 4-11 and 4-12. This group feel that legislation is a good strategy to address their security concerns. This is confirmed when one examines figure 4-9. More than 60% of respondents felt that education as a strategy will reduce identity theft. What is important to note is that adequate legislation regarding personal information protection has already been passed. One such legislation is the Electronic Communications and Transactions Act of 2002. Consumers are however, not knowledgeable about these legislations as indicated in figures 4-10, 4-11 and 4-12. The results in these figures indicate that more than half the respondents have little or no knowledge of consumer protection legislation. Awareness and education will therefore play an important role in this regard.

Almost 80% of respondents disagreed with the statement "Ever since I became a victim of identity theft, I stopped shopping online." The possible reasons are as follows:

- The respondents do not shop online for other reasons and not necessarily because they are a victim of identity fraud. One possible explanation is that customers may not have the facilities (such as a computer system and internet) to shop online.
- The respondents feel that online shopping will not make their life any easier as only 38% responded agreed with this statement.

Clearly, most customers most customers have concerns regarding their personal information security. Legislation has been passed to address these concerns but the study indicates that customers are not knowledgeable about these legislations as indicated in figures 4-10, 4-11, and 4-12. It is, however, imperative that they become knowledgeable about these legislations for their benefit.

4.10 Results on consumer attitudes regarding their personal information protection

This section presents the results of the investigation into the respondents' attitudes toward their personal information protection. An analysis of the results follows.

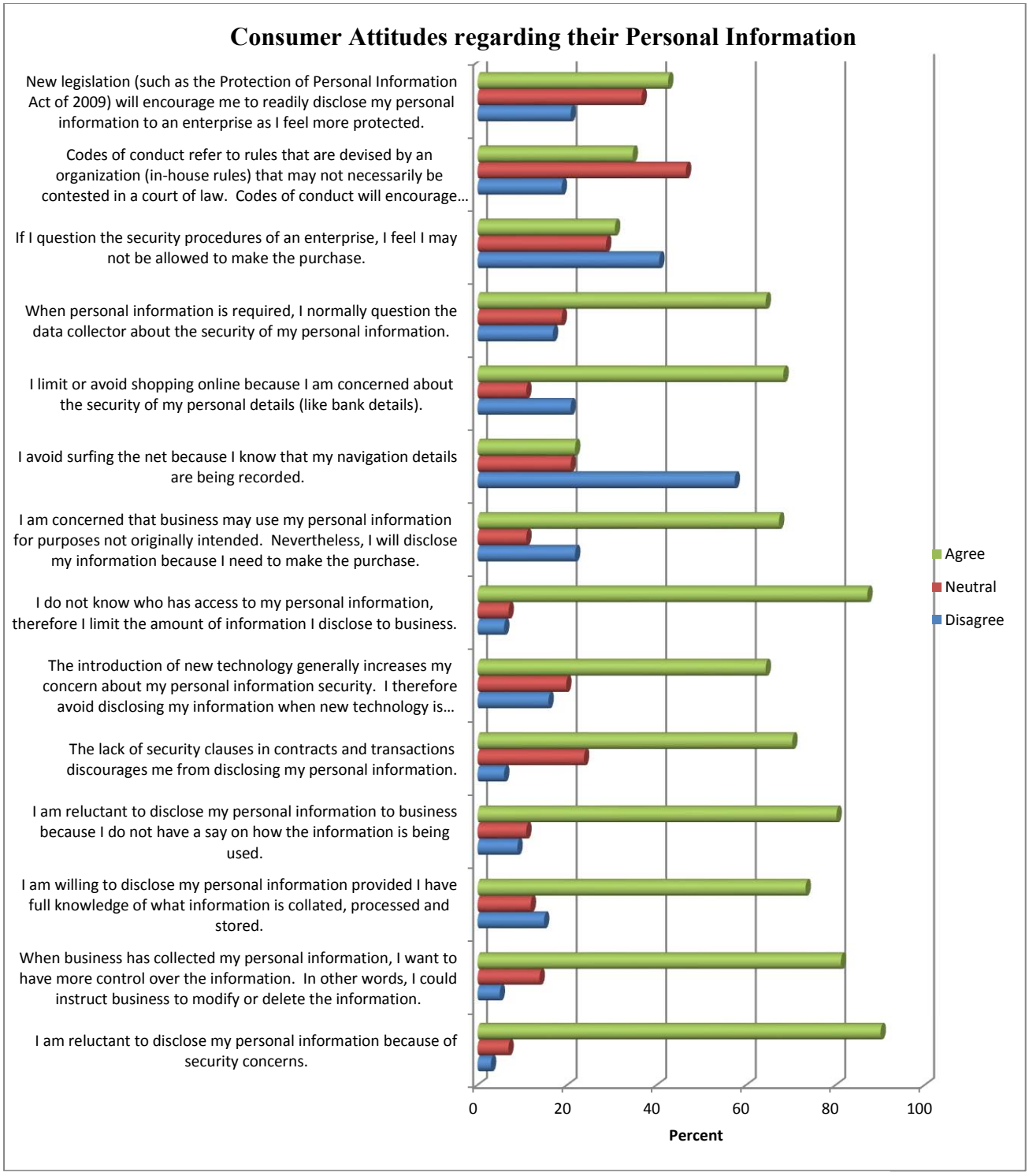


Figure 4-8: Respondents attitudes on their personal information security

For most of the statements, the respondents are more in agreement than disagreement. This indicates that there is a high level of concern amongst respondents about the security of their personal information security. This is in keeping with studies conducted in the area of

consumer concerns. The areas of concern identified in the studies are (Castaneda *et al*. 2007):

- Collection of the information (referred to as "collect").
- Use of the information (referred to as "use").
- Online transactions.

The dimension "collect" relates to how safe the information is with the data collector after it has been collected from the consumer. The dimension "use" relates to whether the information that is collected is used for the intended purpose only (Castaneda *et al*. 2007). Figure 4-7 shows that at least 65% of respondents are concerned that business will use their personal information for other purposes not originally intended. Close to 80% of respondents are reluctant to disclose their personal information to business as they do not have a say on how the information is being used. More than 80% of consumers feel that they do not know who has access to their personal information once it has been disclosed to business. Therefore they limit the amount of information they provide to business. On the other hand 70% of respondents will readily disclose their personal information to business provided that they have full knowledge of what information is collated, processed and stored. Consumers also want to have more control over the information they provide to business. At least 80% of respondents feel that they should be in a position to instruct business to modify the information or completely delete the information in their possession.

One of the aims of legislation is to provide certainty to consumers that their personal information will be protected when they are transacting online (Protection of Personal Information Bill 2009). This certainty should therefore encourage consumers to willingly surrender their personal information to business, but this is not the case as indicated in the figure 4-8 above. The results indicate that only 40% of respondents will readily disclose their personal information to business although legislation is available for their protection. Close to 70% of the respondents either limit or avoid shopping online because they are concerned that personal information like bank details can be intercepted when transacting online. One of the aims of legislations is to encourage consumers to transact online and thereby increase ecommerce activities. The results however indicate that customers are reluctant to transact online because of security concerns. The reluctance to disclose personal information and transact online could be attributed to the fact that more than 50% of respondents are not knowledgeable about the legislations for their protection as indicated in figures 4-10, 4-11

and 4-12. The graphs indicate that more than half the respondents have little or no knowledge of consumer protection legislation.

Close to 60% of respondents disagreed with the statement "I avoid surfing the net because I know my navigation details are being recorded." On the other hand, the results generally indicate that customers are aware that their personal information can be intercepted when transacting online. This is because 60% agreed with the statement "I limit or avoid shopping online because I am concerned about the security of my personal information (like bank details)". It seems, however, that most are ignorant that their navigation details can be intercepted (while surfing the net) yet at the same time they are aware that their personal information can be intercepted when transacting online. These two viewpoints seem to be in contradiction with each other because personal information is generally not required when surfing the net while personal information is always required when transacting online. One can therefore conclude most users prefer surfing the net rather than use the internet for online transactions.

4.11 Results on Legislation, Awareness, Education and Security Issues

It is important to ascertain the opinions of respondents on whether the strategies adopted by government will be successful in reducing identity theft. The result of the investigation is presented in the following graph followed by an analysis.

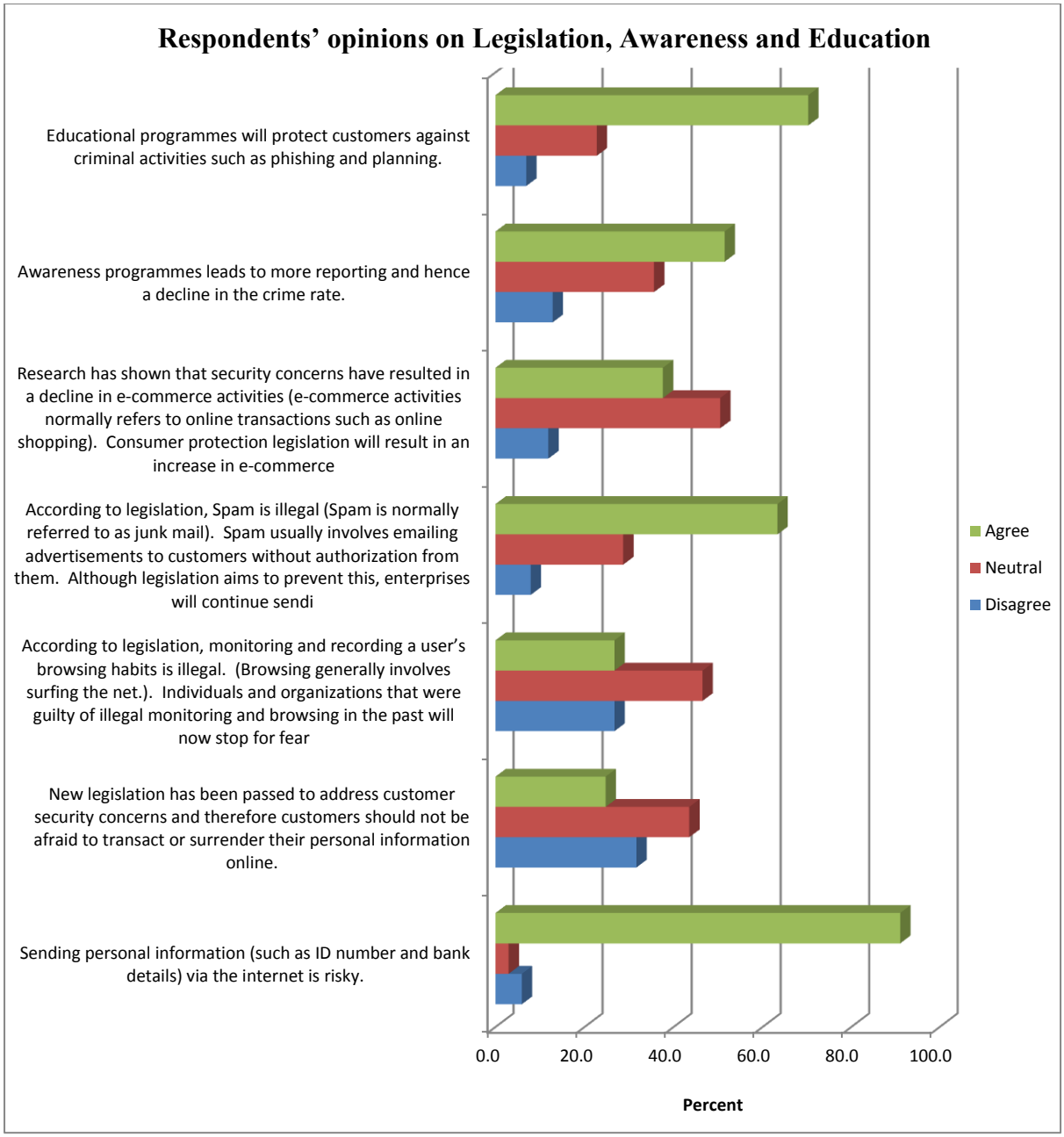


Figure 4-9: Strategies such as Legislation, Awareness and Education

This section elicits the views of respondents on legislation, education and awareness as strategies to reduce identity fraud. At least two thirds (66%) of respondents agree that educational programmes will protect consumers against criminal activities such as phishing and pharming. Studies have shown that educating the consumer about personal information security will help reduce identity theft (Srivastava 2010). The framework proposed by Jamieson *et al* (2008) in section 3.5.3 therefore includes education as an important government strategy to address identity theft crimes (Jamieson *et al*. 2008).

Half the respondents (50%) agree that awareness leads to more reporting and hence a decline in the crime rate. When new consumer protection legislation is passed, the media will have articles in magazines and newspapers making the public aware of the steps they should take when violations take place (Romanosky *et al*. 2008). An increase in media attention will result in more victims coming forward to report identity theft crimes. According to Romanosky *et al* (2008), the media's role is as follows:

- To educate customers about their rights when violations have taken place.
- To increase customer awareness. An increase in awareness will lead to an increase in reporting of any violations.

The net effect is a reduction in identity theft and data breaches.

Less than 40% of respondents felt that new legislation will increase e-commerce activities and only 20% agreed that new legislation will address customers' security concerns. This means that more than 60% of respondents are sceptical about the effectiveness of legislation in reducing identity theft. They are sceptical about whether legislation can be used as a motivation to increase e-commerce activities. This scepticism is also evident when the results regarding illegal monitoring and recording as well as the results regarding Spam are examined. Sixty percent (60%) of respondents agreed that legislation will not stop individuals and business from carrying out illegal monitoring and recording of individuals browsing habits. More than 60% also agreed that although business may be aware that Spam is illegal, they (business) will not be deterred from sending Spam to consumers.

4.12 Respondents awareness of important consumer protection legislation

This section focuses on the third research question. The third research question investigates what level of knowledge respondents have regarding the following:

- Electronic Communications and Transactions Act of 2002.
- Consumer Protection Act of 2008.
- Protection of Personal Information Bill of 2009.

4.12.1 Electronic Communications and Transactions Act of 2002

This section discusses the results of the respondents' knowledge on the Electronic Communications and Transactions Act of 2002. Important pieces of legislations are chosen

from this Act and the consumers' knowledge and awareness regarding this legislation is tested.

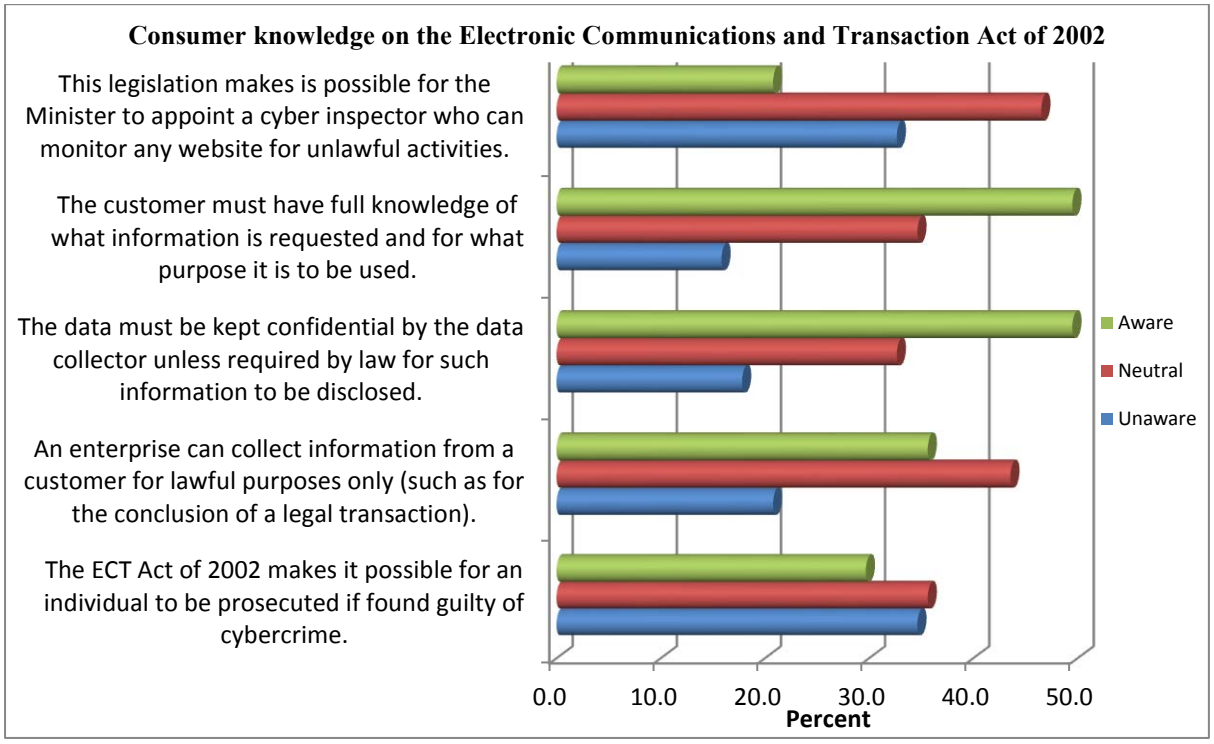


Figure 4-10: Consumer knowledge on The Electronic Communications Act of 2002

Although this is a fairly old legislation, more than half the respondents are unaware about the important aspects of this law. The graph shows a generally low level of awareness on this legislation. For every statement less than half (50%) of respondents have only some knowledge about this important legislation. This means that the majority of customers are either unaware or neutral about this legislation.

Only one fifth (20%) of respondents are aware that the Minister of Communications can appoint a cyber inspector to monitor websites that engage in unlawful activities. It is also notable that less than half (less than 50%) of the respondents are aware that they are entitled to have full knowledge of what information is requested and for what purpose this information is to be used. A fairly small percent (35%) are aware that the information collected can only be used for lawful purposes such as the conclusion of a transaction. Only 28% are aware that cybercrime is a criminal activity and the perpetrator can either be fined or spend time in prison. This is not surprising as it is more difficult to prosecute a perpetrator for cybercrime as compared to more common crimes like house breaking and hijacking (Romanosky *et al*. 2008). The graph also shows that there are about 40% of respondents that

are neutral on most of the statements. This neutrality means there is also much uncertainty amongst respondents about this legislation.

Studies have shown that educating the consumer about consumer protection legislation will help reduce data breaches by business (Jamieson *et al*. 2008). It is therefore imperative that customers become educated about legislation that will protect them.

4.12.2 The Consumer Protection Act of 2008

This section discusses the results of the respondents' knowledge on The Consumer Protection Act of 2008. This Act focuses on the legislative boundaries within which a supplier can operate.

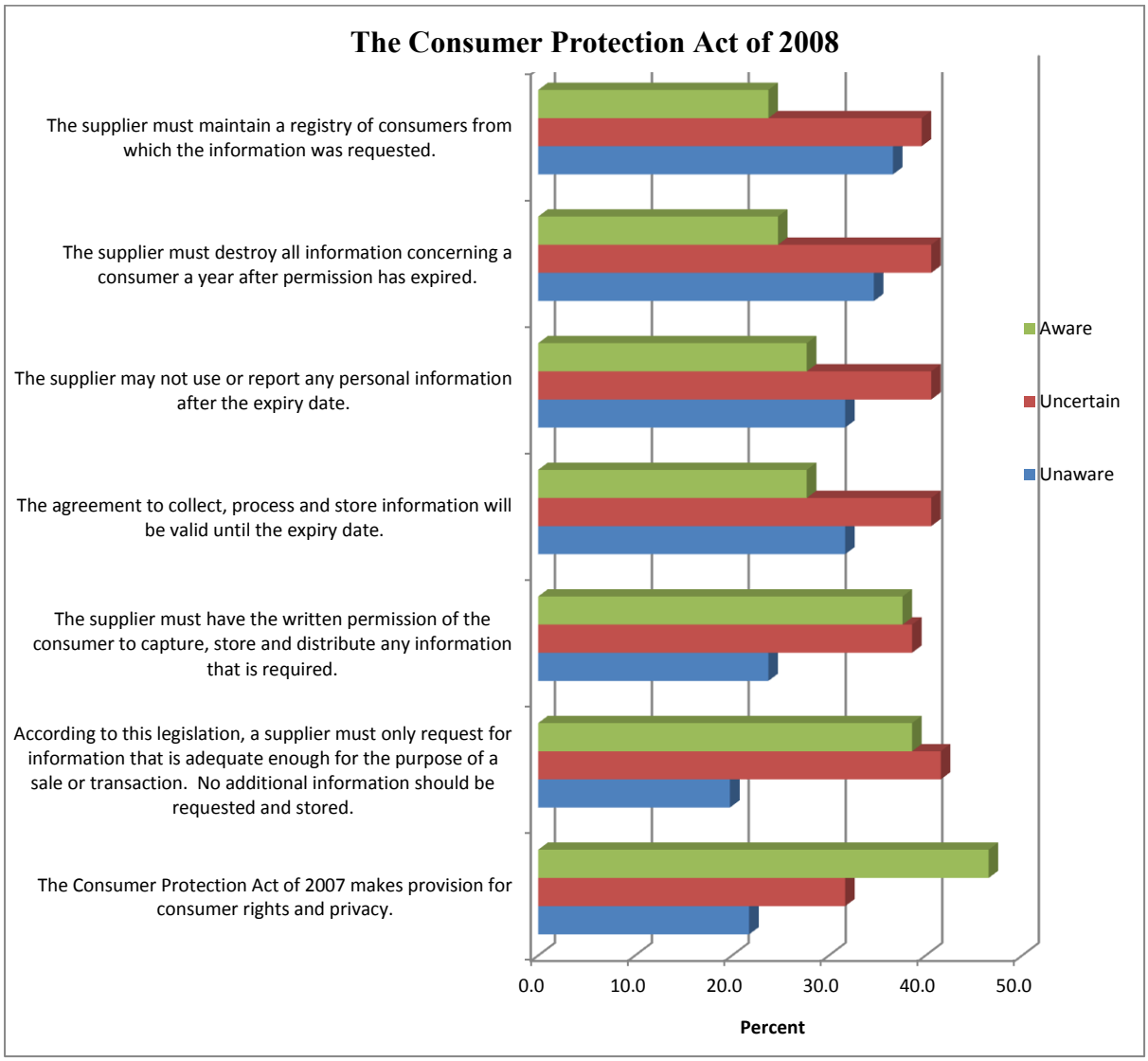


Figure 4-11: Consumer knowledge on The Consumer Protection Act of 2008

The graph shows a generally low level of awareness on this legislation. For every statement, less than 50% of respondents have some knowledge of this important legislation. Also, the graph shows a high level of uncertainty or unawareness about important sections in this legislation. Forty five (45%) responded that they are aware that this Act makes provision for consumer rights and privacy. This is the highest level of awareness when compared to the other statements.

One of the concerns governments have is that a supplier generally requests more information necessary for the conclusion of a transaction (Castaneda *et al*. 2007). This could lead to abuse of consumers' personal information such as using the additional data to carry out surveys or some analysis. The Consumer Protection Act of 2008 makes this illegal. Less that 40% of respondents are aware of this.

This legislation makes it mandatory for a supplier to delete the customers' information one year after the conclusion of a contract. The supplier may not use or report any personal information after the expiry date. This means that the consumer can go back to the supplier to check whether his or her data has been deleted (The Consumer Protection Act of 2008). However, only 25% of respondents are aware that they have the right to do this.

The Consumer Protection Act of 2008 focuses on the boundaries within which a supplier can operate and it is imperative that consumers are aware of these boundaries.

4.12.3 The Protection of Personal Information Bill of 2009

The results of consumers' knowledge on the Protection of Personal Information Bill of 2009 is discussed a nd a nalysed. This is the latest legislation re garding pe rsonal information security and is also the most important for consumers.

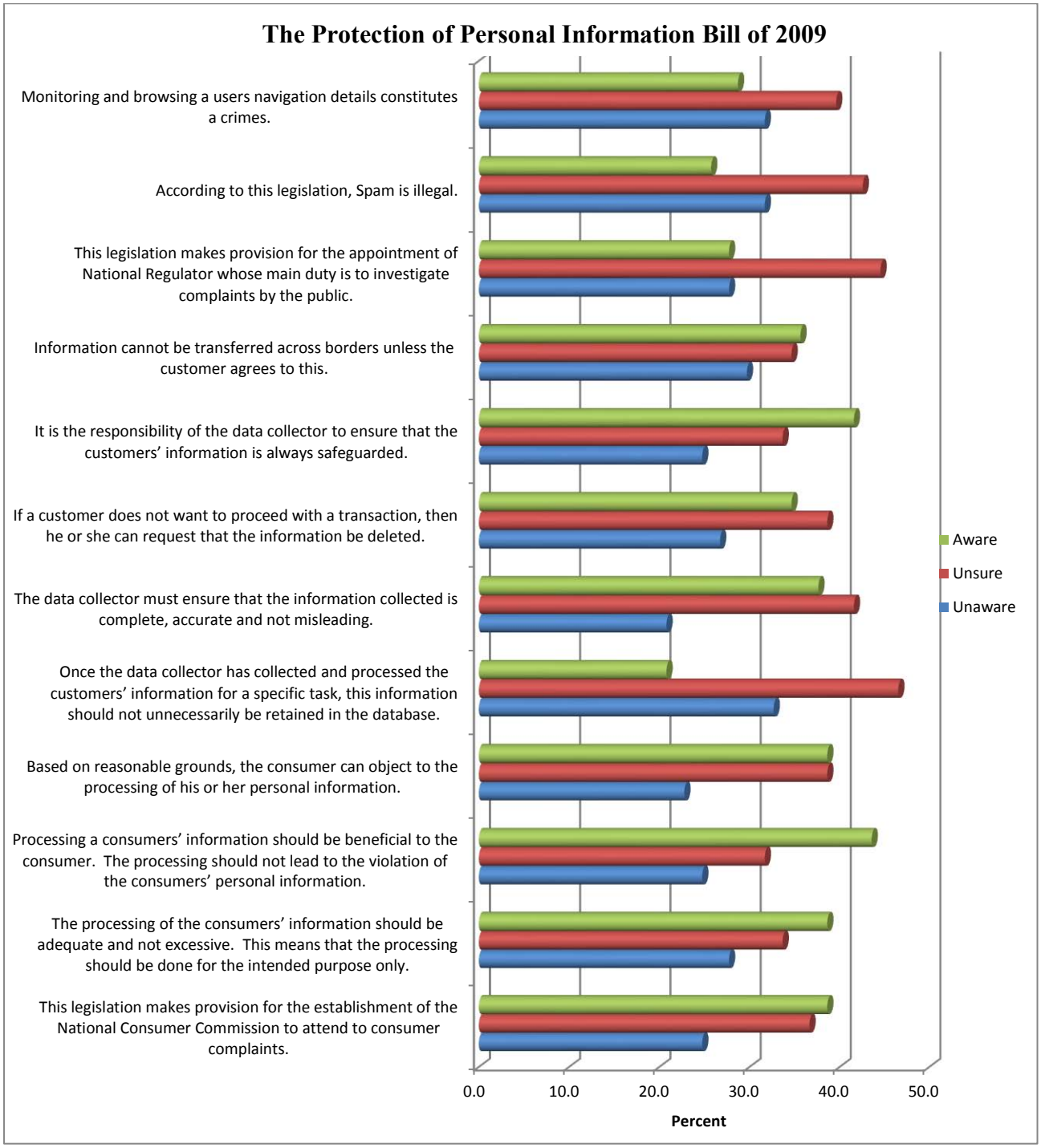


Figure 4-12: Consumer knowledge on the Protection of Personal Information Bill of 2009

This graph shows a generally low level of awareness on the Protection of Personal Information Bill of 2009. This is a similar trend when one examines figures 4-10 and 4-11. Also, less than 50% of respondents have some knowledge of this important legislation. This means that the majority of customers are unaware or uncertain of important sections of this legislation.

There is also a high level of uncertainty for most of the statements. On average, nearly 40% of respondents were uncertain for each question and almost 35% of respondents were totally unaware for each question. Close to 45% of respondents were uncertain that complaints regarding personal information violations could be taken up with the National Regulator. This is important knowledge to have as a law enforcement agency such as the South African Police may not have the expertise to prosecute when data breaches occur. It is the National Regulator who will decide whether to prosecute or not (Protection of Personal Information Bill 2009). A similar percent of respondents were uncertain about the fact that once a transaction had been processed by a business enterprise, the data of the consumer should not unnecessarily be retained in the database. If the consumer is knowledgeable about this then he or she has the right to question the data collector on whether data is being unnecessarily stored after the conclusion of the transaction.

This proposed legislation also has an important section which states that based on reasonable grounds, a consumer can object to the processing of his or her personal information (Protection of Personal Information Bill 2009). The Protection of Personal Information Bill of 2009 gives the customer the freedom to cancel a transaction or contract if he or she has reasonable grounds for doing so. Less than 40% indicated that they have knowledge of this.

One of the concerns consumers have relate to the fact that their personal information will be used illegally for purposes not originally intended (Castaneda *et al*. 2007). Less than 45% were knowledgeable of the fact that excessive processing of an individuals' information is illegal. This means that the processing should be done for the intended purpose only and no other.

This is the latest and most important legislation that deals with the personal information protection of consumers. It is therefore important that strategies such as awareness campaigns and education be used to educate the customer in this legislation.

4.13 Conclusion

This chapter discussed the quantitative results of the investigation that was conducted on the permanent staff at Durban University of Technology. The results are presented in cross tabulations, figures and graphs. The researcher also conducted a detailed analysis of the results showing trends which were compared to theories. Based on the results and analysis, a summary with recommendation is provided in chapter 5.

Chapter 5

SUMMARY AND RECOMMENDATIONS

5.1 Introduction

This chapter presents an overview of the study conducted. Based on the findings, the importance of organizations having security policies to address the security concerns of customers is discussed. This chapter also provides recommendations on how education and awareness drives can be effectively used to address the security concerns of customers so that they (customers) may embrace technology without being concerned about security issues. The chapter concludes by providing recommendations on how present legislation can be improved to address cybercrimes.

5.2 Objectives of the study

The main objective of the study was to investigate how legislation addresses the customers' concerns regarding their personal information security and how knowledgeable they (customers) are on these legislations. The study also investigated the customer's attitude towards their personal information security. The study adopted a quantitative approach using structured questionnaires to reach the objectives.

5.3 Findings and discussions

This section provides a discussion on the findings of the quantitative study done on staff at the Durban University of Technology.

The answer to the main objective of the study is provided in table 4-3. Studies indicate that customers are concerned about the security of their personal information after it has been collected by an organization (Castaneda *et al*. 2007). Customers are also concerned that their personal information can be stolen and used illegally when transacting online (Online Banking Concerns 2011). Pearson's Chi Square test was used to determine how legislation addresses these concerns of customers. The Chi Square test was used to test how significant the relationship between customers' concerns, legislation, security and education are in order to achieve the main objective of the study. Values ≤ 0.05 are considered significant. The Chi Square results indicate that there are significant relationships for 58% of the cross tabulation statements regarding the security concerns of customers and legislation. Most of the security

questions showed significant relationships with legislation as well as illegal monitoring and recording of customers' personal information. Of particular significance is that all 14 questions showed significant relationships with Spam. Customers regard Spam as an invasion of their privacy and a threat to the security of their personal information (What are the effects of Computer Hacking? 2010).

The questions relating to the disclosure of personal information to business showed significant relationship with legislation. This means that customers' want legislation to make it possible for them to have full knowledge of what information is collated and stored. Customers also want to control the information that is collected by business. In other words, they must be allowed to modify or delete any information that is incorrect or incomplete. Customers are also concerned that business will use the information they have collected for purposes not originally intended and they want legislation to protect them in this regard. Legislation has been passed which makes provision for these concerns (The Electronic Communications and Transactions Act of 2002). Customers are, however, generally not knowledgeable about these legislations as indicated in figures 4-10, 4-11 and 4-12. It is recommended that businesses in South Africa adopt policies to address the security concerns of customers as indicated in the results. Some companies (outside South Africa) have already adopted policies formulated from information protection legislations. The researcher could not find any South African company that has a comprehensive security policy based on legislations. The policy of the National Bank of Canada is therefore used as an example. The National Bank of Canada is one such company that has practices and policies based on the Protection and Electronic Documents Act (Principles of Consumer Protection for Electronic Commerce, A Canadian Framework 1999). Some of the principles enshrined in their policy are:

- Accountability to their clients. This includes the management of the information with proper security procedures to protect the information. The Protection of Personal Information Bill of 2009 (South African legislation) also has a section that specifies that the data collector is responsible for the management and security of information collected (Hofmeyr 2011).
- The legislative boundaries within which the organization operates are fully adhered to. After consent has been given by the clients for the collection of the information, they (the clients) are informed about the purpose for collecting the information. Only the minimum amount of information required for the conclusion of a transaction is

collected. Clients can have access to their personal information to check and correct the information. The principles of the National Bank of Canada therefore give clients full control of the information they have collected. When the results in table 4-3 and figure 4-8 are examined, respondents also expressed their desire to have knowledge and control of the information that is collected by an organization.

It is therefore recommended that companies in South Africa use the example of the National Bank of Canada to formulate similar policies. The National Bank of Canada is used as an example because their policy is closely related to principles enshrined in South African legislations regarding personal information security. The Consumer Protection Act of 2008 (South African legislation) provides the legislative boundaries within which a company can operate when collecting and using the personal information of customers (Consumer Protection Act 2008). This legislation however falls short in making it mandatory for companies to formulate policies on personal information security. It is therefore hoped that future legislations will compel companies to formulate policies that affect the security of customers' personal information.

The aim of legislation is to provide confidence to customers that they should not be afraid to transact online because they are protected by legislation (Protection of Personal Information Bill 2009). The results show that there is a significant relationship between most of the questions on customer concerns and legislation. The results therefore confirm that legislation is an important strategy in addressing the security concerns of consumers.

The second objective of the study was to test the respondents' knowledge on customer protection legislations. The results regarding customers' awareness of the Electronic Communications and Transactions Act of 2002 are depicted in figure 4-10. The results indicate that only one fifth (20%) of respondents are aware that the Minister of Communications can appoint a cyber-inspector to monitor websites that engage in unlawful activities. It is important to note that less than half (less than 50%) of the respondents are aware that they are entitled to have full knowledge of what information is requested and for what purpose this information is to be used. A fairly small percent (35%) are aware that the information collected can only be used for lawful purposes such as the conclusion of a transaction. Only 28% are aware that cybercrime is a criminal activity and the perpetrator can either be fined or spend time in prison. The results also indicate that there are about 40%

of respondents that are neutral on most of the statements. This neutrality means there is also much uncertainty amongst respondents about this legislation.

The results regarding customers' awareness of The Consumer Protection Act of 2008 are depicted in figure 4-11. Here, the role of the supplier was focussed upon. These questions tested the consumers' knowledge on the legislative boundaries within which the supplier can operate. The results indicate a generally low level of awareness on this legislation. For every statement, less than 50% of respondents have some knowledge of this important legislation. Also, the results indicate a high level of uncertainty in most of the statements. This means that the majority of customers are unaware about important sections of this legislation. Forty five (45%) responded that they are aware that this Act makes provision for consumer rights and privacy. This is the highest level of awareness when compared to the other statements.

One of the concerns governments have is that a supplier generally requests more information necessary for the conclusion of a transaction (Castaneda *et al*. 2007). This could lead to abuse of consumers' personal information such as using the additional data to carry out tasks not originally intended. The Consumer Protection Act of 2008 makes this illegal. Less that 40% of respondents are aware of this.

The Consumer Protection Act of 2008 makes it mandatory for a supplier to delete the customer's information one year after the conclusion of a contract. The supplier may not use or report any personal information after the expiry date. This means that the consumer can go back to the supplier and check whether his or her data has been deleted (The Consumer Protection Act of 2008). However, only 25% of respondents are aware that they have the right to do this.

Respondents were also tested on their knowledge of The Protection of Personal Information Bill of 2009. The results are depicted in figure 4-11. When this Bill is passed in parliament in 2011, it will become the latest legislation regarding personal information security. It will also become the most important legislation for consumers. The results indicate a generally low level of awareness on this Bill. This is a similar trend when one examines figures 4-10 and 4-11.

There is also a high level of uncertainty for most of the statements. Close to 45% of respondents were uncertain that complaints regarding personal information violations could be taken up with the National Regulator. A similar percent of respondents were uncertain

that once a transaction had been processed by a business enterprise, the data of the consumer should not unnecessarily be retained in the database.

This proposed legislation also has an important section which states that based on reasonable grounds, a consumer can object to the processing of his or her personal information (Protection of Personal Information Bill 2009). The Protection of Personal Information Bill of 2009 gives the customer the freedom to cancel a transaction or contract if he or she has reasonable grounds for doing so. Less than 40% indicated that they have knowledge of this.

The Electronic Communications and Transactions Act of 2002, the Consumer Protection Act of 2008 and the Protection of Personal Information Bill of 2009 are the most important legislation that deals with customer protection. The results of the study indicate that consumers generally have little or no knowledge of these legislations (as indicated in figures 4-10, 4-11 and 4-12). It is therefore recommended that education and awareness campaigns be launched to educate individuals about these legislations. According to the results in figure 4-9, most respondents agreed that awareness and education are important strategies that should be employed to reduce identity theft. Education and awareness campaigns have been successfully implemented in some communities. The researcher decided to present a discussion on two communities where such campaigns are implemented. The first discussion focuses on a highly technologically advanced community in the state of Maine in the United States of America. The second discussion focuses on an awareness campaign implemented in a district called Vhembe in Venda (South Africa) where technology and broadband internet access is available but needs to be upgraded and sustained. These two studies are chosen because they represent the two diverse facets of Internet technology in South Africa i.e. regions that are highly technologically advanced as well as regions where internet technology needs to be vastly improved.

The campaign in Maine was called the National Cyber Security Awareness Campaign Challenge (Castigliola 2010). McAfee, a company that specializes in cyber security also endorsed the campaign. The primary focus of this campaign was to educate residents and businesses about cybercrime prevention. The campaign also aimed to reduce undue fear of cybercrimes by providing accurate information about risks. Information regarding the awareness campaign was done online and individuals were encouraged to participate via a channel called My Maine Privacy. Individuals openly discussed Internet safety and privacy awareness. Participants were educated about safe habits to be adopted when communicating

or transacting online. The secondary benefit of such a campaign is that other communities will use this initiative as an example to launch similar drives. The campaign expects to reduce identity theft to less than the norm of 35% in the state of Maine. It is recommended that similar education and awareness drives be implemented (in South Africa) in regions where users have constant access to internet facilities so that such campaigns can be conducted online.

A campaign was also carried out in the district of Vhembe (South Africa). Research conducted by the Council for Scientific and Industrial Research in conjunction with the University of Venda indicated that the local communities are not equipped to deal with cyber attacks (Grobler, van Vuuren & Zaaiman 2010). To address this issue, a pilot project was initiated in the district of Vhembe to educate volunteers at the University of Venda about the following:

- Physical security: This training involves the importance of securing the physical computer by protection mechanisms such as passwords.
- Malware: Volunteers are educated about the different types of malware that are encountered in cyberspace and how to protect the computer against malware attacks.
- Safe surfing: This session teaches volunteers about safe internet surfing, email security as well as safety precautions to be taken during file sharing, downloads and storing of information.
- Social aspects of cyber security: Volunteers are taught about the safe ways of using social networking. They are also educated about identity theft, cookies and cyber bullies.

The volunteers participating in this course are current students as well past graduates. Individuals who are working in the Information Technology environment have also been encouraged to enrol for this course. After completing the course, the volunteers are expected to go back to their communities and educate computer users about cybercrimes and what steps they should adopt to minimize such crimes. By embarking on such education and awareness campaigns, it is hoped that the personal information security of internet users is enhanced. Business should also take the initiative in having similar campaigns to address cybercrimes. The initiatives by business will help protect the image of the organization as individuals lose faith in companies that experience breaches (Ranger 2007).

There are many factors that serve as a motivation to consider education and awareness drives as strategies to address cybercrimes. The following are the most important ones:

- Many businesses are already experienced phishing attacks. One such attack was aired in the popular programme called Carte Blanche on 23 January 2011 (Christoforou and Comrie 2011). The programme focussed on phishing attacks on Standard Bank clients.
- The number of people using internet for online transactions have increased. Consequently, there has been an increase in identity theft (Srivastava 2010).
- The government has expressed the need for all citizens to have access to ICT (Information and Communication Technology) (Grobler *et al*. 2010). When this becomes possible, more internet users will become vulnerable to cyber attacks.

In the light of the above, the government and business should take the responsibility of protecting citizens against cyber attacks. Awareness and education campaigns are therefore important strategies that must be considered. Such campaigns will encourage the user to adopt safer habits when transacting or communicating online. This will lead to greater protection of their personal information and the potential for online users becoming victims of a cyber-attack is also reduced. By not implementing such campaigns, the South African Internet infrastructure will become vulnerable to attacks by cyber terrorists (Fourie 2007) and this may have an impact on national security (Grobler *et al*. 2010).

The third objective of the study was to investigate the respondents' attitudes toward their personal information security. The results are depicted in figure 4-8. For most of the statements, the respondents are more in agreement than disagreement. This indicates that there is a high level of concern amongst respondents about the security of their personal information security. Close to 80% of respondents are reluctant to disclose their personal information to business as they do not have a say on how the information is being used. More than 80% of consumers feel that they do not know who has access to their personal information once it has been disclosed to business. Therefore they limit the amount of information they provide to business. On the other hand, it is interesting to note that 70% of respondents will readily disclose their personal information to business provided that they have full knowledge of what information is collated, processed and stored. At least 80% of respondents feel that they should be in a position to instruct business to modify or completely delete the information in their possession.

One of the aims of legislation is to provide certainty to consumers that their personal information will be protected when they are transacting online (Protection of Personal Information Bill 2009). This certainty should therefore encourage consumers to willingly surrender their personal information to business, but this is not the case as indicated in figure 4-8. The results indicate that only 40% of respondents will readily disclose their personal information to business although legislation is available for their protection. Close to 70% of the respondents either limit or avoid shopping online because they are concerned that personal information like bank details can be intercepted when transacting online. The aim of the Protection of Personal Information Bill of 2009 is to encourage customers to transact online and thereby increase ecommerce activities. The results indicate that this is not happening because of security concerns. The reluctance to disclose personal information and transact online could be attributed to the fact that more than 50% of respondents are not knowledgeable about the legislations for their protection as indicated in figures 4-10, 4-11 and 4-12. The results indicate that more than half the respondents have little or no knowledge of consumer protection legislation.

The results also indicate that most are ignorant that their navigation details can be intercepted (while surfing the net) yet at the same time they are aware that their personal information can be intercepted when transacting online. These two viewpoints seem to be in contradiction with each other because personal information is generally not required when surfing the net while personal information is always required when transacting online. One can therefore conclude that most users prefer surfing the net rather than use the internet for online transactions.

It is therefore recommended that businesses formulate policies (similar to the policies of the National Bank of Canada) to address the security concerns of customers. These policies should also allow customers to have control of their personal information. The importance of implementing the recommendation (i.e. business having security policies) is that customers will feel confident that their personal information is secure in the hands of business and that they (customers) can also have control of the information collected. Organizations that have strong security policies experience fewer breaches and customers will associate themselves with such organization (Ranger 2007). This may also lead to more customers transacting online with such organizations. An increase in online transactions means an increase in income for companies and the fiscal income of the state will also increase. It is therefore important that governments and business take steps to encourage customers to embrace

technology and transact online. Legislation, education and awareness are therefore important strategies that should be adopted by the government and business.

5.4 A broad overview on legislation as strategy to reduce identity theft

The researcher found that South Africa has adequate legislations to address the security concerns of customers. The main concern of customers is that their personal information is stolen when transacting online (Online Banking Concerns 2011). The Protection of Personal Information Bill of 2009 has sections that address these concerns. South African legislations on personal information security compares favourably with similar legislations in the European Union and the United States. There are however some shortcomings. South African legislation on personal information protection is very broad and does not have specific sections regarding Spam, cyber stalking, the use of password sniffers, the creation and the writing of viruses and website defacements. Most states in the United States of America have however specific sections in its legislations that address these types of cybercrimes (Cassim 2009). The 95/46/EU directive of the European Union also has a section dedicated to Spam. It makes the distribution of unsolicited emails to individuals a criminal offence (Castaneda *et al*. 2007). Having specific sections in the legislation for different types of cybercrimes means that cybercriminals will be put into various categories according to the crimes committed. This will help in the prosecution process. It is therefore recommended that the broad principles regarding personal information security (in South Africa) be formulated into sections that specifically address the different types of cybercrimes. Since phishing has become the most common method of internet identity theft (Srivastava 2007), the United States of America has passed the Anti-Phishing Act of 2004 that defines phishing as a federal felony (Laws that protect the internet from phishing, Congress and Phishing 2004). Phishing is the main method used by cyber criminals to steal the personal information of online users in South Africa (Christoforou and Comrie 2011). It is therefore recommended that South Africa follow the example of the United States of America by having legislation that specifically deals with phishing to address this type of cybercrime. South African legislation has adequate guidelines regarding the boundaries within which business should operate when dealing with the personal information of customers (The Consumer Protection Act 2008). The Consumer Protection Act of 2008 however falls short in recommending what penalties business should receive if they are found guilty of any transgressions regarding the security of customer's personal information (The Protection of Personal Information Bill 2009). It is therefore recommended that legislation

be passed that specifies what punishment an enterprise should receive when they are found guilty of compromising the personal information of customers. This will serve as an example to other enterprises that are deliberately compromising the personal information of customers.

Although there are shortcomings in South African legislations regarding personal information protection, customers feel protected by present legislations as indicated in figure 4-9. It is hoped that these shortcomings will be addressed in subsequent legislations.

5.5 Suggestions for future research

The following are recommendations for future research:

- In this study, the researcher focussed on respondents from Durban University of Technology. A similar study can be conducted in a business organization, government department or any other organization that has the same or similar objectives as this study. The results of the study in various organizations may differ depending on the nature of the organization. The results of the study on employees of an IT company for example (where employees may be more knowledgeable about information security) may differ from the results of employees from a call centre (where the tasks of employees may be operational). The organization may require information about their employees' knowledge and attitude regarding their personal information security before embarking on awareness campaigns (similar to the one discussed in section 5.3).
- One of the recommendations in section 5.3 is that education and awareness campaigns should be initiated in the community to address cybercrimes. If such campaigns are undertaken, it would be beneficial to carry out research that investigates the extent to which cybercrimes are reduced as a result of these drives.
- New legislations (especially the Consumer Protection Act of 2008) have created boundaries within which business must operate. Future research should investigate the extent to which businesses are adhering to the principles enshrined in consumer protection legislations.

5.6 Limitations of the study

There are many approaches that can be adopted with regards to information security. The most important ones are government regulation, self-regulation and third-party regulation (a combination of the first two approaches). Government regulations rely on judicial and

legislative processes. Self-regulation puts the onus on the private sector (such as private business enterprises) to protect customers. This may take the form of codes of conduct and security clauses based on legislation. A third-party approach adopts an independent but trusted third party to assume the responsibility for protecting customers. The limitation of this study is that only government regulations were focussed upon because most countries are adopting this approach to protect its citizens. Although self-regulation and third-party approaches are not very popular, these approaches are being adopted by some countries like the US. This study however did not focus on these two approaches because of limited statistics and literature available. It is therefore not clear whether these approaches are more effective than government regulation.

There were also limitations regarding the statistics used in this study. Although the main focus of the study is on how security issues (on personal information) of the South African consumer can be addressed, statistical information from the UK and the US was used to indicate that identity fraud is of a serious concern. It would therefore have been more appropriate to use statistical information in a South African context if such information was available.

There are also some limitations regarding the research methodology. The population for this study are the personnel at DUT who are generally computer literate. The questionnaire was however not distributed to respondents who have limited computer knowledge. If a similar study was carried out in other organizations, the results of the study may therefore differ depending on the nature of the organization and the computer literacy level of respondents. Another limitation is that The Protection of Personal Information Bill has not been enacted as yet and it was not clear whether respondents could appropriately answer questions on this Bill.

5.7 Conclusion

This study examined the legislative Acts and Bills that are available for protecting customers against the illegal interception and use of their personal information. The study indicated that South Africa has adequate legislation to address the security concerns of customers. Customers agreed that legislation is an important government strategy that should be adopted by government. The study also researched respondents' knowledge about these legislation. The results indicated that customers are generally uncertain or unaware about most sections of current legislation that affect them. The researcher has therefore recommended that

awareness and education campaigns be adopted by government and business to educate customers about their personal information protection. The study also investigated customers' attitudes regarding their personal information security. The results indicated that customers are unwilling to transact online because of concerns regarding illegal monitoring and interception on the Internet. They also expressed concerns on issues relating to SPAM. The results indicated that customers are willing to surrender their personal information to business provided they are protected by legislation. They also want to have control over the information that is collected by business.

References

Aaron, R. 2010. *Phishing Statistics* (online). Available WWW: http://www.brighthub.com/internet/.../99607.aspx/ (Accessed 5 March 2011).

Akinsuyi, F. 2005. *Combating Identity theft* (online). Available WWW: http://www.dataflows.com/common/.../Combating%20Identity%20Theft.pfd (Accessed 20 April 2011).

AlAwadhi, S. and Morris, A. 2009. Factors Influencing the Adoption of E-government Services. *Journal of Software*. 4(6): 584-594.

Al-qdah, M. and Hui, L.Y. 2011. Simple Encryption/Decryption Application. *International Journal of Computer Science and Security*. 1(1): 33-40.

Anderson, K. B, Durbin, E., Salinger, M. A. 2008. Identity Theft. *Journal of Economic Perspectives*. 22(2): 171-192.

Brody, R. G., Mulig, E., Kimball, V. 2007. Phishing, Pharming and Identity Theft. *Academy of Accounting and Financial Studies Journal*. 11(3): 43-56.

Bryman, A. 2004. *Social Research Methods*. United States: Oxford University Press.

Buttarelli, G. 2010. *Data protection legislation in Europe, preventing cyber-harassment by protecting personal data and privacy*. European Data Protection Supervisor, 07 June 2010.

Cassim, F. 2009. Formulating specialized legislation to address the growing spectre of cybercrime: a comparative study. *Potchefstroomse Elektroniese Regsblad*. 12(4): 2-31.

Castaneda, J. A., Montoso, F. J., Luque, T. 2007. The dimensionality of customer privacy concern on the internet. *Online Information Review*. 31(2): 420-439.

Christoforou, A. and Comrie, S. 2011. *Phishing* (online). Available WWW: http://beta.mnet.co.za/carteblanche/Article.aspx?id=43330&showid=5 (Accessed 10 May 2011).

Clossum, R. M. 2010. *Information Privacy: A Quantitative Study of Citizen Awareness, Concern and Information Seeking Behaviour Related to the Use of the Social Security Number as a Personal Identifier*. Master's Thesis, University of Tennessee.

Cyber crime unit saves UK economy £140m in six months (online). 2011. Available WWW: http://www.guardian.co.za/uk/2011/oct/02/cyber-crime-unit-met-police (Accessed 10 October 2011).

Data Protection Directive (online). 2011. Available WWW: http://en.wikipedia.org/wiki/Data_Protection_Directive (Accessed 12 January 2011).

Davis, F. D. 1989. Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly*. 13(3): 39-340.

Denial of service (online). 2011. Available WWW: http://searchsoftwarequality.techtarget.com/definition/denial-of-service (Accessed 20 June 2011).

Doll, W. J., Henddrickson, A., Deng, X. 1998. Using Davis's Perceived Usefulness and Ease of Use Instruments for Decision Making: A Confirmation and Multi-Group Invariance Analysis. *Decision Science*. 29(4): 839-869.

Ecommerce critical components (online). 2008. Available WWW: http://smallbusinessbible.org/ecommerce_cri.../ (Accessed 15 March 2011).

Electronic Commerce (online). 2011. Available WWW: http://e..wikipedia.org/wiki/ECommerce/ (Accessed 15 August 2011).

Firewalls (online). 2011. Available WWW: http://www.referenceforbusiness.com/small/Eq-Inc/Firewalls.html (Accessed 15 February 2011).

Fourie, I. 2007. Cyber Terrorism: Political and Economic Implications. *Online Information Review*. 31(2): 242-243.

Fraud: awareness and prevention (online). 2011. Available WWW: http://cml.org.uk/cml/policy/issues/3658 (Accessed 10 March 2011).

Gibbs, E. 2011. *Say No to Hackers and Spyware 2011* (online). Available WWW: http://saynotohackersandspyware.blogspot.com/ (Accessed 15 April 2011).

Grobler, M., van Vuuren, J., Zaaiman, J. 2011. *Evaluating cyber security awareness in South Africa*. Proceedings of the 10th European Conference on Information Warfare and Security.

The Institute of Cybernetics at the Tallinn University of Technology, Tallinn Estonia, 7-8 July 2011.

Hardin, A. M., Chang, J. C., Fuller, M. A., Torkzadeh, G. 2010. Formative Measurement and Academic Research: In Search of Measurement Theory. *Educational and Psychological Measurement*. 71(1): 281-305.

Hofmeyr, C. 2011. *Doing Business in South Africa* (online). Available WWW: http://www.cliffedekkerhofmeyer.com/news/invest/ecommerce.htm (Accessed 10 May 2011).

How To Avoid Getting Hooked By Pfishing (online). 2004. Available WWW: http://www.identity-theft-tips.com/how-to-avoid-getting-hooked-by-pfishing/ (Accessed 6 October 2010).

Howard, A. 2011. *Identity Theft Stories Reveal How Victims can be arrested* (online). Available WWW: http://ezinearticles.com/?Identity-Theft-Stories-Reveal-How-Victims-Can-Be-Arrested&id (Accessed 15 June 2011).

Identity Theft and Identity Fraud (online). 2011. Available WWW: http://gae-rproxy.appspot.com/EjryZmxvwlfhZzzz/http/criminal/fraud/websites/idtheft.html (Accessed *20* May 2011).

Identity Theft Expert (online). 2009. Available WWW: http://identitytheftexpert.co.za/ (Accessed 12 January 2011).

Igbaria, M., Guimaraes, T., Davis, G. B. 1995. Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems*. 11(4): 87-14.

Information Security (online). 2011. Available WWW: http://en.wikipedia.og/wiki/information_security (Accessed 12 February 2011).

Jamieson, R., Land, L., Stephens, G., Winchester, D. 2008. Identity Crime: The Need for an Appropriate Government Strategy. *Forum on public Policy*. Spring: 1-23.

Johnson, A. 2005. *The Technology Acceptance Model And The Decision To Invest In Information Security.* Proceedings of the 2005 Southern Association of Information Systems Conference. North Carolina Agricultural and Technical State University. United States of America.

Johnson, A. and Bhattacharyya, G. K. 2006. *Statistics: Principles and Methods*. United States of America: John Wiley and Sons.

Kim, G. W., Lee, D. G., Han, J. W., Lee, S. H., Kim, S. W. 2009. Security technology based on a home gateway for making smart homes secure. *Internet Research*. 19(2): 209-226.

Kyl, J. 2000. *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions* (online). 2000. Available WWW: http://www.privacyrights.org/ar/id_theft.htm (Accessed 12 December 2010).

Lang, M., Devitt, J., Kelly, S., Kinneen, A., O'Malley, J., Prunty, D. 2009. *Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland* (online). Available WWW: http://www.computer.org/portal/web/csdl/doi/10.1109/ICMeCG.2009.105 (Accessed 23 May 2011).

Laws that protect the Internet from phishing, Congress and Phishing (online). 2004. Available WWW: http://www.anti-phishing.info/congress-and-phishing.htm (Accessed 20 October 2010).

Lederer, A. L., Maupin, D. J., Sens, M. P., Zuang, Y. 2000. The technological acceptance model and the World Wide Web. *Decision Support Systems*. 29(3): 269-282.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., Kvasny, L. 2009. Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*. 9(3): 155-172.

Malhotra, N. K., Kim, S. S., Agarwal, N. K. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*. 15(4): 336-355.

Mann, J. 2010. *Moscow gets tough on cybercrime as ID theft escalates* (online). Available WWW: http://www.ft.com/cms/s/0/04e59450-3552-11df-9cfb-001444feabdc0.html (Accessed 25 April 2011).

Manos, S. 2011. *Difficult to enforce Cyber and American Cyber Competitive Act of 2011* (online). Available WWW: http://...wordpress.com/.../difficult-to-enforce (Accessed 3 April 2011).

Margulis, S. T. 1997. Conceptions of Privacy: Current Status and the Next Steps. *Journal of Social Issues*. 33(3): 5-21.

Mitchell, V. W. 1999. Consumer perceived risk: conceptualizations and models. *European Journal of Marketing*. 33(12): 163-195.

Mohan, R. 2011. *Trademark Disputes Over Domain Names* (online). Available WWW: http://bukisa.com/.../429772_trademark-disp.../ (Accessed 8 March 2011).

Multipoint Strategy to Fight Cybercrime (online). 2010. Available WWW: http://www.mcafee.com/us/campaigns/fight_cybercrime/strategy.html (Accessed 12 July 2011).

National Cybersecurity Awareness Campaign Challenge: My Maine Privacy. (online). 2010. Available WWW: http://www.castigliola.com/index.php?option=com_content...id (Accessed 15 July 2010).

Nwaocha, V. O. 2010. Protecting Consumers from the Menace of Phishing. *International Journal of Computing and Network Security*. 2(10): 59-63.

Online Banking Concerns (online). 2011. Available WWW: http://ww.ehow.com/list_6728621_online-banking-concerns.html (Accessed 1 July 2011).

Operating infrastructure (online). 2009. Available WWW: https://sustainability.standardbank.com/economic-performance/operating-infrastructure/ (Accessed 5 October 2011).

Petter, S., Straub, D., Rai, A. 2007. Specifying Formative Constructs in Information Systems Research. *MIS Quarterly*. 31(4): 623-656.

Pharming (online). 2011. Available WWW: http://wwwmysecurecyberspace.com/...pharming (Accessed 23 march 2011).

Principles of Consumer Protection for Electronic Commerce, a Canadian Framework (online). 1999. Available WWW: http://strategis.ic.gc.ca/oca (Accessed 12 April 2011).

Privacy and Human Rights 2003: Overview (online). 2003. Available WWW: http://www.privacyinternational.org/survey/phr2003/overview.htm (Accessed 15 January 2011).

Privacy and Human Rights 2003: South Africa (online). 2003. Available WWW: http://www.privacyinternational.org/survey/phr2003/countries/southafrica.htm (Accessed 20 May 2011).

Prosecutors say Kansas man facing federal tax charges tried to flee overseas (online). 2011. Available WWW: http://www.jworld.com/news/2011/apr/07/prosecutors-say-kansas-man-facing-feder (Accessed 8 June 2011).

Ranger, S. 2007. *"Data breach laws make companies serious about security"* (online). Available WWW: http://management.silicon.com/itdirector/0,39024673,39168303,00.htm?r=1 (Accessed 12 March 2011).

Reducing the Risk of Identity Theft (online). 2010. Available WWW: http://www.gs.gov.nl.ca/consumer/consumer_affairs/ident_en.html (Accessed 13 March 2011).

Regulation of Interception of Communications and Provision of Communication-Related Information Act (online). 2010. Available WWW: http://...wikipedia.org/.../regulation_of_Inter (Accessed 15 April 2011).

Republic of South Africa. 2007. *The Consumer Protection Act, No.68 of 2008.* Pretoria: Government Printer.

Republic of South Africa. 2002. *The Electronic Communications and Transactions Act, No. 25 of 2002*. Pretoria: Government Printer.

Republic of South Africa. 2009. *Protection of Personal Information Bill, No. 32495 of 2009.* Pretoria: Government Printer.

Romanosky, S., Telang R., Acquisti, A. 2008. *Do Data Breach Disclosure Laws Reduce Identity Theft?* (online). Available WWW: www.networkworld.com/newsletters/2008/072808sec1.html (Accessed 30 December 2010).

Safeena, R., Abdulla, K.M., Date, H. 2010. Customer Perspectives on E-business Value: Case Study on Internet Banking. *Journal of Internet Banking and Commerce*. 15(1): 1-13.

Safeena, R., Date, H., Kammani, A. 2011. Internet Banking Adoption in an Emerging Economy: Indian Consumer's Perspective. *International Arab Journal of e-Technology*. 2(1): 56-64.

Scamwatch (online). 2011. Available WWW: http://www.scamwatch.gov.au/content/index.phtml/tag/Nigerian419Scams (Accessed 9 May 2011).

Seldon, A. 2009. *E-Business in South Africa, a matter of trust* (online). Available WWW: http://netdotwork.co.za/article.aspx?pklarticleid=3081 (Accessed 16 January 2011).

Shahzad, A., Naseem, R., Aadil, F., Khayyam, S. 2010. Trends in defensive techniques against Denial of Service (DoS) Attacks. *Canadian Journal on Network and Information Security*. 1(1): 25-33.

Siciliano, R. 2011. *Survey Shows Account Takeover Fraud Drops* (online). Available WWW: http://www.finextra.com/community/fullblog.aspx?i.../ (Accessed 28 February 2011).

Srivastava, P. 2010. *Online Shopping and Security now go hand in hand!* (online). AvailableWWW: http://www.techprocess.co.in/pdf/Nov10/Audiencematters_29_Nov_2010.pdf (Accessed 15 March 2011).

Srivastava, T. V. 2007. *Phishing and Pharming-The Evil Twins* (online). Available WWW: http://www.sans.org/reading_room/whitepapers/privacy/ (Accessed 10 January 2011).

Stewart, C. 2004. *Online Security Tips & Tools* (online). Available WWW: http://www.identity-theft-tips.com/online-security-tips-tools (Accessed 6 October 2010).

Stone, A. 2010. "Patient records for all to see". *The Daily Dispatch* (online), April 25. Available WWW: http://news.za.msn.com/local/article.aspx?cp-documentid=153155730 (Accessed 30 April 2010).

Sund, C. 2007. Towards an international road-map for cybersecurity. *Online Information Review*. 31(5): 566-582.

Tanfa, D.Y. 2006. *Advance Fee Fraud*. Phd. Thesis, University of South Africa.

TechWeb. 2006. TechEncyclopedia (online). Available WWW: http://techweb.com/encyclopedia/ (Accessed 2 January 2011).

Thompson, C. 1999. If you could just provide me with a sample: examining sampling in qualitative and quantitative research papers. *Evid Based Nurs.* 2(3): 68-70.

Volio, F. 1981. *Legal personality, privacy and the family: The International Bill of Rights*. New York: Columbia University Press.

Welman, C., Kruger, F., Mitchell, B. 2009. *Research Methodology.* 3rd ed. South Africa: Oxford University Press.

What are the effects of Computer hacking (online). 2010. Available WWW: http://www.guard-privacy-and-online-security.com/what-are-the-effects-of-computer- (Accessed 28 March 2011).

What is an IP Address? (online). 2011. Available WWW: http://whatismyipaddress.com/ip-address (Accessed 15 January 2011).

What is Credit Card Fraud? (online). 2001. Available WWW: http://www.fraudscreening.com/What IsFraud.html (Accessed 28 March 2011).

Why is cyber crime hard to prosecute? (online). 2009. Available WWW: http://answers.yahoo.com/question/index?qid=20090428211257AAIUHEk (Accessed 23 March 2011).

Wright, K. 2005. Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services. *Journal of Computer-Mediated Communication.* 10(3): 1-18.

Zimerman, M. 2011. The dangers of malware in a library computing environment. *The Electronic Library.* 29(1): 5-19.

Zondo-Kabini, H. 2003. Application of the Communications and Transactions Act to Online Merchants from Other Jurisdictions. *Northwestern Journal of Technology and Intellectual Property.* 1(1): 1-7.

ANNEXURE A: Questionnaire

Title: **Personal Information Security: Legislation, Awareness and Attitude**

Section A: Background

Business requires personal identifiable information (PII) such as ID number, e-mail address and bank account details from customers. Research has shown that customers are concerned about the security of their personal information especially when they are transacting online.

Legislation has been put in place to address the security concerns of customers. One such example is The Electronic Communications and Transaction Act of 2002. The aim of this Bill is to protect customers against fraudulent activities on the internet. Awareness and education is also encouraged to minimize identity theft. The researcher is therefore interested in investigating the following:

- The customers' attitude towards their personal information protection.
- The views of customers on strategies (such as legislation, awareness and education) to address these security concerns.
- The customers' knowledge of information security legislation.

Indicate your choice with an X.

Section B: General Questions

Choose one of the following options:

1. **Gender:**
   Male ☐ Female ☐

2. **Age:**
   18-24 ☐ 25-34 ☐ 36-60 ☐ over 60 ☐

3. **Status:**
   Lecturer ☐ Senior Lecturer ☐ Professor ☐
   Other (such as Secretary, Librarian, Maintenance worker, etc) ☐

4. **Faculty:**
   Engineering ☐ Arts ☐ Economic and Management Sciences ☐
   Accounting and Informatics ☐ Health Sciences Other ☐ ☐

5. **Location:**

Durban ☐ Pietermaritzburg ☐

6. Do you own a shopping card (such as an Edgars card) or a credit card?
Yes ☐ No ☐

6.1 If you choose the option "Yes", then answer the following questions.

Shopping and credit card information	**Strongly Agree**	**Agree**	**Neutral (Not Sure)**	**Disagree**	**Strongly Disagree**
a) I use my card every time I make a purchase					
b) I use my card only when I run out of cash.					
c) I will only use my card in an emergency.					

6.2 If you choose the option "No", then answer the following questions.

Shopping and credit card information	**Strongly Agree**	**Agree**	**Neutral (Not Sure)**	**Disagree**	**Strongly Disagree**
a) I did not apply for a shopping or credit card because personal information (such as bank details) is required and I am concerned about the security of this information.					
b) I feel that owning a shopping or credit card is risky because someone can fraudulently use my credit card details to make purchases.					
c) Credit card information can be intercepted when transacting online and this will compromise the security of my personal information. Therefore I am not motivated in owning a shopping or credit card.					

7. Do you shop online?

Yes ☐ No ☐

7.1 If you choose "Yes" as an option, then answer the following questions.

Information on online shopping	**Strongly Agree**	**Agree**	**Neutral (Not Sure)**	**Disagree**	**Strongly Disagree**
a) I shop online because it is convenient.					
b) Shopping online is cheaper.					
c) I shop online because I have never been a victim of identity theft.					
d) If I become a victim of identity theft, I will stop shopping online.					
e) If I become a victim of identity fraud, I will continue shopping online because the bank will take responsibility for my losses.					
f) Although there are security risks involved when I shop online, I am not concerned about these risks because I feel safe with new consumer protection laws.					
g) Although I am concerned about Internet associated risks, I still shop online.					

7.2 **If you choose the option "No", then answer the following question.**

Information on online shopping	**Strongly Agree**	**Agree**	**Neutral (Not Sure)**	**Disagree**	**Strongly Disagree**
a) I do not shop online because I do not have the facilities (such as a computer system and internet).					
b) I am afraid to shop online because individuals can gain access to my personal information and make illegal purchases.					
c) Ever since I became a victim of identity theft, I stopped shopping online.					
d) I do not shop online because current legislation is not adequate for my personal information security.					
e) I will only shop online once adequate consumer protection legislation becomes available.					
f) I feel that online shopping will not make my life easier and therefore I am not interested.					

Section C: Questions on Consumer Attitudes regarding their personal information security.

Attitude criteria regarding consumers' personal information security	**Strongly Agree**	**Agree**	**Neutral (Not Sure)**	**Disagree**	**Strongly Disagree**
1. I am reluctant to disclose my personal information because of security concerns.					
2. When business has collected my personal information, I want to have more control over the information. In other words, I could instruct business to modify or delete the information.					
3. I am willing to disclose my personal information provided I have full knowledge of what information is collated, processed and stored.					
4. I am reluctant to disclose my personal information to business because I do not have a say on how the information is being used.					
5. The lack of security clauses in contracts and transactions discourages me from disclosing my personal information.					
6. The introduction of new technology generally increases my concern about my personal information security. I therefore avoid disclosing my information when new technology is introduced.					
7. I do not know who has access to my personal information, therefore I limit the amount of information I disclose to business.					
8. I am concerned that business may use my personal information for purposes not originally intended. Nevertheless, I will disclose my information because I need to make the purchase.					
9. I avoid surfing the net because I know that my navigation details are being recorded.					
10. I limit or avoid shopping online because I am concerned about the security of my personal details (like bank details).					
11. When personal information is required, I normally question the data collector about the security of my personal information.					
12. If I question the security procedures of an enterprise, I feel I may not be allowed to make the purchase.					

13. Codes of conduct refer to rules that are devised by an organization (in-house rules) that may not necessarily be contested in a court of law. Codes of conduct will encourage me to disclose my personal information.					
14. New legislation (such as the Protection of Personal Information Bill of 2009) will encourage me to readily disclose my personal information to an enterprise as I feel more protected.					

Section D: Questions on Legislation, Awareness, Education and Security Issues

Legislation, Awareness, Education and Security Issues	**Strongly Agree**	**Agree**	**Neutral (Not Sure)**	**Disagree**	**Strongly Disagree**
1. Sending personal information (such as ID number and bank details) via the internet is risky.					
2. New legislation has been passed to address customer security concerns and therefore customers should not be afraid to transact or surrender their personal information online.					
3. According to legislation, monitoring and recording a user's browsing habits is illegal. (Browsing generally involves surfing the net.). Individuals and organizations that were guilty of illegal monitoring and browsing in the past will now stop for fear of prosecution.					
4. According to legislation, Spam is illegal (Spam is normally referred to as junk mail). Spam usually involves emailing advertisements to customers without authorization from them. Although legislation aims to prevent this, enterprises will continue sending Spam.					
5. Research has shown that security concerns have resulted in a decline in e-commerce activities (*e-commerce* activities normally refers to online transactions such as online shopping). Consumer protection legislation will result in an increase in *e-commerce* activities.					
6. Awareness programmes lead to more reporting and hence a decline in the crime rate.					
7. Educational programmes will protect customers against criminal activities such as phishing and planning.					

Section E: This section will test the respondents' knowledge of the Electronic Communications and Transactions Act of 2002

Electronic Communications and Transactions Act of 2002	**Am fully aware of this**	**Am aware of this but more clarity is needed**	**Not sure (may have read or heard about this)**	**Generally unaware of this although I may have heard or read about this**	**Am totally unaware of this**
1. The ECT Act of 2002 makes it possible for an individual to be prosecuted if found guilty of cybercrime.					
2. An enterprise can collect information from a customer for lawful purposes only (such as for the conclusion of a legal transaction).					
3. The data must be kept confidential by the data collector unless required by law for such information to be disclosed.					
4. The customer must have full knowledge of what information is requested and for what purpose it is to be used.					
5. This legislation makes is possible for the Minister to appoint a cyber inspector who can monitor any website for unlawful activities.					

Section F: This section will test the respondents' knowledge of The Consumer Protection Act of 2008

The Consumer Protection Act of 2008	**Am fully aware of this**	**Am aware of this but more clarity is needed**	**Not sure (may have read or heard about this)**	**Generally unaware of this although I may have heard or read about this**	**Am totally unaware of this**
1. The Consumer Protection Act of 2008 makes provision for consumer rights and privacy.					
2. According to this legislation, a supplier must only request for information that is adequate enough for the purpose of a sale or transaction. No additional information should be requested and stored.					
3. The supplier must have the written permission of the consumer to capture, store and distribute any information that is required.					
4. The agreement to collect, process and store information will be valid until the expiry date.					
5. The supplier may not use or report any personal information after the expiry date.					
6. The supplier must destroy all information concerning a consumer a year after permission has expired.					
7. The supplier must maintain a registry of consumers from which the information was requested.					

Section G: This section will test the respondents' knowledge of the Protection of Personal Information Bill of 2009

The Protection of Personal Information Bill of 2009	**Am fully aware of this**	**Am aware of this but more clarity is needed**	**Not sure (may have read or heard about this)**	**Generally unaware of this although I may have heard or read about this**	**Am totally unaware of this**
1. This legislation makes provision for the establishment of the National Consumer Commission to attend to consumer complaints.					
2. The processing of the consumers' information should be adequate and not excessive. This means that the processing should be done for the intended purpose only.					
3. Processing a consumers' information should be beneficial to the consumer. The processing should not lead to the violation of the consumers' personal information.					
4. Based on reasonable grounds, the consumer can object to the processing of his or her personal information.					
5. Once the data collector has collected and processed the customers' information for a specific task, this information should not unnecessarily be retained in the database.					
6. The data collector must ensure that the information collected is complete, accurate and not misleading.					
7. If a customer does not want to proceed with a transaction, then he or she can request that the information be deleted.					
8. It is the responsibility of the data collector to ensure that the customers' information is always safeguarded.					
9. Information cannot be transferred across borders unless the customer agrees to this.					
10. This legislation makes provision for the appointment of National Regulator whose main duty is to investigate complaints by the public.					
11. According to this legislation, Spam is illegal.					
12. Monitoring and browsing a users navigation details constitutes a crimes.					

ANNEXURE B CRONBACH'S ALPHA

Cronbach's alpha measures how well a set of items (or variables) measures a single uni dimensional latent construct. When data have a multidimensional structure, Cronbach's alpha will usually be low. Technically speaking, Cronbach's alpha is not a statistical test - it is a coefficient of reliability (or consistency).

Cronbach's alpha can be written as a function of the number of test items AND the average inter-correlation among the items. Below, for conceptual purposes, we show the formula for the standardized Cronbach's alpha:

$$\alpha = \frac{N \cdot \bar{c}}{\bar{v} + (N-1) \cdot \bar{c}}$$

Here N is equal to the number of items, c-bar is the average inter-item covariance among the items and v-bar equals the average variance.

One can see from this formula that if you increase the number of items, you increase Cronbach's alpha. Additionally, if the average inter-item correlation is low, alpha will be low. As the average inter-item correlation increases, Cronbach's alpha increases as well.

This makes sense intuitively - if the inter-item correlations are high, then the items are measuring the same underlying construct. This is really what is meant when someone says they have "high" or "good" reliability. They are referring to how well their items measure a single unidimensional latent construct.

Thus, if you have multi-dimensional data, Cronbach's alpha will generally be low for all items. In this case, run a factor analysis to see which items load highest on which dimensions, and then take the alpha of each subset of items separately.

ANNEXURE C CHI SQUARE TEST

A chi-square test is any statistical hypothesis test in which the test statistic has a chi-square distribution when the null hypothesis is true, or any in which the probability distribution of the test statistic (assuming the null hypothesis is true) can be made to approximate a chi-square distribution as closely as desired by making the sample size large enough.

Specifically, a chi-square test for independence evaluates statistically significant *differences* between proportions for two or more groups in a data set.

Chi-square test statistic:

$$\chi^2 = \frac{(f_o - f_e)^2}{f_e}$$

$$df = (r-1)(c-1)$$

ANNEXURE D Informed Consent form to participants

UNIVERSITY OF KWAZULU-NATAL
SCHOOL OF INFORMATION SYSTEMS AND TECHNOLOGY

Dear Respondent,

MCom Research Project
Researcher: Steven Parbanath (Cell Number: 0845055278)
Supervisor: Professor M Maharaj (Office Telephone Number: 0312608003)

I, **Steven Parbanath**, am a MCom student, at the School of Information Systems and Technology, of the University of KwaZulu-Natal. You are invited to participate in a research project entitled **Personal Information Security: Legislation, Awareness And Attitude**.

The aim of this study is to investigate:

- The extent to which legislation will address consumer fears regarding personal information protection.
- Customers' attitude towards their personal information protection
- The level of knowledge customers have regarding their personal information protection.

Through your participation I hope to understand the following:

- The level of knowledge customers have on consumer protection legislation.
- The opinions of customers on legislation as a government strategy to reduce identity theft.
- Whether customers will feel more secure with customer protection legislation so that they will be able to embrace technology.
- The attitudes of consumers' regarding their personal information protection.

The results of the survey are intended to contribute to increasing customer knowledge and awareness so that identity theft is reduced.

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Information Systems and Technology, UKZN.

If you have any questions or concerns about completing the questionnaire or about participating in this study, you may contact me or my supervisor at the numbers listed above.

The survey should take you about **20** minutes to complete. I hope you will take the time to complete this survey.

Sincerely

Investigator's signature _____ Date_____

ANNEXURE E Consent form of participant

CONSENT

I……..... (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project.

I understand that I am at liberty to withdraw from the project at any time, should I so desire.

SIGNATURE OF PARTICIPANT DATE

……

ANNEXURE F Ethical Clearance letter

UNIVERSITY OF
KWAZULU-NATAL
University of KwaZulu-Natal
Research Office
Govan Mbeki Centre
Westville Campus
University Road
Chiltern Hills
Westville
3629
South Africa
Tel No: +27 31 260 3587
Fax No: +27 31 260 2384
E-mail : naidoos4@ukzn.ac.za

29 November 2010

Mr S Parbanath
School of Information Systems and Technology
WESTVILLE CAMPUS

Dear Mr Parbanath

PROTOCOL: Personal Information Security: Legislation, Awareness and Attitude
ETHICAL APPROVAL NUMBER: HSS/1370/2010 M: Faculty of Management Studies

In response to your application dated 25 November 2010, Student Number: **201555757** the Humanities & Social Sciences Ethics Committee has considered the abovementioned application and the protocol has been given **FULL APPROVAL.**

PLEASE NOTE: Research data should be securely stored in the school/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

Professor Steve Collings (Chair)
HUMANITIES & SOCIAL SCIENCES RESEARCH ETHICS COMMITTEE

SC/sn

cc: Prof. M Maharaj (Supervisor)
cc: Mrs. C Haddon