Developing a Framework for E-commerce Privacy and Data Protection in Developing Nations: a case study of Nigeria

By

Tiwalade Adelola

A Doctoral Thesis

Submitted in partial fulfilments for the award of Doctor of Philosophy of Loughborough University

2017

Abstract

The emergence of e-commerce has brought about many benefits to a country's economy and individuals, but the openness of the Internet has given rise to misuse of personal data and Internet security issues. Therefore, various countries have developed and implemented cyber-security awareness measures to counter this. However, there is currently a definite lack in this regard in Nigeria, as there are currently, little government-led and sponsored Internet security awareness initiatives. In addition, a security illiterate person will not know of the need to search for these awareness programmes online, particularly in Nigeria's case, where personal information security may not be regarded as an overly important issue for citizens.

Therefore, this research attempts to find a means to reduce the privacy and data protection issues. It highlights the privacy and data protection problem in developing countries, using Nigeria as a case study, and seeks to provide a solution focusing on improving Internet security culture rather than focusing on solely technological solutions.

The research proves the existence of the privacy and data protection problem in Nigeria by analysing the current privacy practices, Internet users' perceptions and awareness knowledge, and by identifying factors specific to Nigeria that influence their current privacy and data protection situation.

The research develops a framework for developing countries that consists of recommendations for relevant stakeholders and awareness training. In the case of Nigeria, the stakeholders are the government and organisations responsible for personal information security, and an awareness training method has been created to take into account Nigeria's unique factors. This training method encompasses promoting Internet security awareness through contextual training and promoting awareness programmes.

Industry experts and Nigerian Internet users validated the framework. The findings obtained from the validation procedure indicated that the framework is applicable to the current situation in Nigeria and would assist in solving the privacy and Internet problem in Nigeria. This research offers recommendations that will assist the Nigerian government, stakeholders such as banks and e-commerce websites, as well as Nigerian Internet users, in resolving the stated problems.

Acknowledgements

I would like to thank my supervisors, Prof. Ray Dawson and Dr. Firat Batmaz, for the patient guidance, support, encouragement and advice throughout my time as a student. I have been extremely lucky to have supervisors who cared about my work and progress. Their patience and support, helped in the realisation of the research goal. I also appreciate Dr. Russell Lock for his annual review on my research progress and advice given.

I am thankful to my parents for their financial support, assistance and for all their encouragement. Undergoing a PhD programme as a fee-paying student is capital intensive and, without their assistance, it would have been impossible to complete this research.

I also appreciate my husband for his support and encouragement especially during the data gathering stage of my research. I would also like to say thank you to my beloved siblings and in-laws for their prayers and support throughout my study. My deepest thanks go to my research colleagues in the Computer Science and other departments at Loughborough University for their advice and support throughout.

I would like to thank, as well, everyone who has contributed and participated in this research including experts, participants and government officials.

Table of Contents

List of Figures

List of Tables

Glossary of Abbreviations

BVN	Bank Verification Number
COBIT	Control Objectives for Information and Related Technologies
CIA	Central Intelligence Agency
DPA	Data Protection Act
DPR	Data Protection Register
E-AP	E-Awareness Portal
ENISA	European Network and Information Security Agency
EU	European Union
FIP	Fair Information Practice
FTC	Federal Trade commission
GDP	Gross Domestic Product
HTTPS	Hypertext Transfer Protocol Secure
HUs	Home Users
ISPs	Internet Service Providers
ICO	Information Commissioner Officer
ISP-ISA	Internet service Provider-information Security Awareness Framework
ISMS	Information Security Management System
NIST	National Institute of Standards and Technology
NITDA	National Information Technology Development Agency
NGO	Non-Governmental Organisations
NHUs	Non-Home Users
OECD	The Organization for Economic Cooperation and Development
PII	Personal Identifiable Information
US	United States
UK	United Kingdom
VPN	Virtual Private Network

List of Publications

Adelola, T; Dawson, R. and Batmaz, F., 2014, Privacy and data protection in E-commerce: The effectiveness of a Government Regulatory Approach in Developing Nations, using Nigeria as a case. In: Paper presented at the 9th international conference for Internet technology and secured transactions (ICITST-2014)

Adelola, T. Dawson, R. and Batmaz, F., 2015, Nigerians' Perceptions Of Personal Data Protection And Privacy, SQM (Software Quality Management) And Inspire (International Conference For Process Improvement, Research And Education) Conference, 30th March 2015.

Adelola, T., Dawson, R., and Batmaz, F., 2015, "Privacy and data protection in e-commerce in developing nations: evaluation of different data protection approaches." The International Journal for Digital Society IJDS.

Adelola, T., Dawson, R., and Batmaz, F., 2015, "The urgent need for an enforced awareness programme to create Internet security awareness in Nigeria." Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services. ACM.

Chapter 1 Introduction

This chapter guides the reader to the motivation for this research by presenting the research problem domain. In addition, it provides an introduction to the thesis and the research topic along with a general background on Internet privacy, data protection and information security.

1.1 Background

Internet users rely more and more on the convenience and flexibility of the Internet to shop communicate and, in general, perform tasks that would otherwise require a physical presence, becoming an indispensable part of the daily life of people in their public and private affairs. Unfortunately, this leaves room for more undesirable issues to surface such as online crime, fraud, and privacy violation (Niranjanamurthy *et al.,* 2013).

Security and privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for e-commerce providers (Niranjanamurthy and Chahar, 2013).

E-commerce, which ordinarily is supposed to be advantageous, particularly to a developing nation's economy, like Nigeria's, could become a source of concern to Internet users due to the high level of cybercrime and lack of initiatives to combat this issue (Ehimen and Bola, 2010). As many instances of cybercrime go unreported, is difficult to give an accurate figure, however evidence from operational agencies suggests that economic costs of cybercrime in Nigeria are substantial (Boniface, Michael and Victor, 2015).

Therefore, it is the responsibility of the website owners to practice good privacy practices in order to ensure customers' information is safe and to improve e-commerce trust. Studies have

shown that trust of online businesses can be enhanced through privacy policies, and by paying attention to the security of private information that is collected (Jakovljević, 2011). A privacy policy is a comprehensive description of a websites' information and privacy practices, usually located in an easily accessible place on the site and these policies are typically the only information source available to consumers (Federal Trade Commission, 2000).

Several countries, such as the United Kingdom and Canada, have enacted legislation and procedures to protect the information privacy of their citizens and corporations (Cate and Mayer-Schönberger, 2013; Jamal, Maier and Sunder, 2005a). However, many developing countries, such as Nigeria, are yet to enact any effective procedures, despite the high level of identity theft and online fraud. The Organisation for Economic Co-operation and Development (OECD) is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade (OECD, 2013). They have played a major role in developing e-commerce data protection principles. Due to the privacy issues, the OECD, the U.S. government and the European Union began extensive discussions about developing a regulatory framework for privacy (Jamal, Maier and Sunder, 2005a).

The European Union in 1995 (Legislation, 2016) decided to adopt formal enforcement in the form of the European Directives incorporating the eight OECD principles, while the United States, although endorsing the principles, adopted the self-regulation approach rather than governmental regulation (Cate and Mayer-Schönberger, 2013).

However, even with the existence of privacy solution to provide adequate security, without the underlying perception and awareness from customers these solutions may not be effective. Most customers are of the opinion that that security is solely the responsibility of a third party, for instance, the government, websites, banks, or IT professionals (Kritzinger and

von Solms, 2010). Internet users need to be educated about information security so that they can protect themselves from these security threats.

According to a Nigerian cyber threat survey (Wolf Park and Digital Jewels, 2014) cybercrime is common in Africa, however it is more prevalent in Nigeria due to the population size, the push towards a cashless society, relatively high Internet penetration, lack of adequate security controls, and weak governance. Furthermore, many Nigerians are unskilled and the high digital illiteracy could pose a significant risk to the state of Internet security in the country (Akanbi and Akanbi, 2012; Tayo, Thompson and Thompson, 2016). This study explores the problem of data protection and Internet privacy in Nigeria and attempts to understand how it hinders the growth, and acceptance of e-commerce as compared to developed countries. It does this by investigating several aspects of privacy policies in Nigerian e-commerce websites in order to understand the general privacy practices in Nigeria and the problems in its privacy practices. The study also examines Nigerian Internet home-users and their lack of Internet security awareness and suggests the need for actively promoting Internet security awareness to cyber-security culture, thereby improving e-commerce adoption and growth.

1.2 Useful Definition of Terms

1.2.1 Definition of Personal Identifiable Information (PII)

Personal identifiable information (PII) is simply any data that could potentially identify a specific individual. PII can be sensitive or non-sensitive. Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. It can be easily gathered from public records, phone books, corporate directories and websites. Sensitive PII is defined as information that if lost, compromised, or disclosed could result in substantial harm or inconvenience to an individual (Rouse, 2014). These include health and medical information, race or ethnicity, political party affiliation, religious beliefs, sexual

orientation, passport, and sensitive financial information (bank account details and credit/debit card details).

As people use e-commerce and the Internet, huge amounts of personal, financial, organisational, and commercial data are being collected, processed automatically, and stored electronically (Tajpour, Ibrahim and Zamani, 2013). Although it is important to protect sensitive information, totally disregarding non-sensitive information would not be advisable. Identity theft is the assumption of another person's identity by using the victim's identifying information (Tajpour, Ibrahim and Zamani, 2013). This information includes sensitive information like their social security number, credit card numbers, and bank account information and non-sensitive information like a person's name, address, and date of birth.

Thompson (2008), a Security Strategist, did an experiment to prove that non-sensitive PII such as name, date of birth or Facebook address could be enough to gain access to more sensitive information. After the experiment, he was able to gain access to a volunteer's email account, which gave him access to the victim's bank account and ultimately had access to the victim's money (Thompson, 2008).

1.2.2 Definition of Privacy

The term privacy has been studied for over 100 years from philosophical, sociological, psychological, and legal perspectives; however, there is no definite description of the term (Smith, Dinev and Xu, 2011). There are numerous definitions of *privacy* in the literature. One of the oldest definitions of privacy was the right to be left alone (Warren and Brandeis, 1890).

Another definition suggests that privacy has two parts: a psychological state and a physical feature of the environment. The psychological part refers to the control of and access to

personal information. The environmental part refers to the technical system or the physical isolation that gives the feeling of privacy (Sundstrom, Burt and Kamp, 1980).

Skinner, Han and Chang (2006) went further in defining and understanding privacy by emphasising that an individual‘s privacy is a human right. Bellotti (1997) summarised privacy as a capability to determine what one wants to reveal and how accessible one wants to be.

In the context of e-commerce, privacy can be defined as an “individual’s right to control their personal information with respect to its collection, use, and transfer by entities engaged in e-commerce” (Boritz and No, 2011). Individuals must disclose personal information to complete e-commerce transactions, however, it can be misused, for example, by sending unwanted emails to customers, selling customers’ information to others, or disclosing potentially sensitive information that the customer would prefer to keep private. Therefore, in such a context, the invasion of privacy is commonly viewed as the unauthorised collection, use, and transfer of personal information as a direct result of e-commerce transactions (Milberg, Smith and Burke, 2000).

Privacy and data protection are closely linked but they should not be considered identical. Generally, data protection has a privacy dimension but it is narrower in scope than the privacy concept, “as privacy covers all issues relating to the protection of an individual's personal space” i.e. private life, private home, private correspondence and so on. (Veghes *et al.,* 2009). From a different angle, data protection encloses a wider area, since personal data are protected not only to enhance the privacy of the subject, but also to guarantee other fundamental rights, such as the right to freedom of expression, the right to know what data is gathered about you, to have access to your data, to ask for modification or deletion of your data, and so on. (European Commission, 2009).

1.3 Statement of Research Problem

Various studies have stated that privacy and security is one of the main concerns for successful e-commerce implementation (Adkinson, Eisenach and Lenard, 2002; Antón, Earp and Reese, 2002). The Internet enables people to share their personal information, but Internet users are prone to security attacks. Collection and processing of personal data is not a problem by itself. Internet businesses use the data to profile customers and deliver suitable personalised services. These data are collected by asking consumers directly or indirectly, or from third parties (Lee, Ahn and Bang, 2011).

These activities have raised the concern as to the security of the information being transferred, especially when it involves personal details such as their real name, credit card details and bank account details. Millions of adults have been reported becoming cybercrime victims every day (Symantec Norton, 2012; Furnell, Tsaganidi and Phippen, 2008). Researchers also agree that even though a website uses the best technical solution to provide adequate security, without the underlying perception and awareness from customers, these solutions may be ineffective (Kritzinger and Smith, 2008). Africa has huge potential and promise, and yet struggles to break the vicious circle of poverty. Nonetheless, Internet penetration in Africa has greatly increased over the last half decade from to 2015 (Internet Live Stats, 2015) with the prevailing poor infrastructures, limited human resources, poor governance and inadequate initiatives leaving African Internet users highly vulnerable (Borena, Belanger and Egigu, 2015). Existing research confirms the security concern about e-commerce in Nigeria, due to a general lack of awareness of cyber threats and an increase of online retail stores and e-commerce activity (Wolf Park and Digital Jewels, 2014). Yet, the current literature rarely mentions these privacy aspects and protection mechanisms in Africa, creating a knowledge gap on the matter (Borena, Belanger and Egigu, 2015). It is important

to understand the background setting of developing countries in order to effectively apply initiatives established in developed countries to them. Therefore, it is necessary to examine the present situation in Nigeria and give recommendations based on the findings of the research.

1.4 Research Scope

The research investigated current e-commerce privacy and security issues in Nigeria and further determined the current websites' privacy practices. A study of Nigerian Internet users' perception of data protection and privacy was also conducted. Although the technical solutions are essential to defend against Internet security and privacy issues, more focus was made on human factors such as awareness and self-regulation as a solution to reduce the security issues. The research underlines the problem of e-commerce Internet privacy and security in Nigeria used as an example of a developing country. It seeks to understand the factors that affect the e-commerce privacy and security issues in such a society and to propose a solution to enhance Nigerian's awareness of these issues through an effective awareness framework and improve the websites' privacy practices.

1.5 Research Aim and Objectives

The main aim of the research is to identify and develop strategies that will enhance e-commerce privacy and data protection in developing nations. This should improve trust issues regarding performing transactions online and inevitably improve e-commerce adoption in developing nations.

The objectives that have to be met to fulfil the objectives are:

1. To review literature on previous and related work in the research area to see what has already been done to identify the e-commerce data protection and privacy problems in

developing countries, and in Nigeria in particular, and to identify what approaches have been adopted in developed countries and in Nigeria.

2. To determine the effectiveness of the approaches used in developed nations in a developing nation by evaluating the United Kingdom's Information Commissioner's Office (ICO) dispute resolution, enforcement and compliance monitoring processes for their applicability in Nigeria.

3. To confirm the existence of a problem in the e-commerce privacy and data protection approach in Nigeria by analysing websites' privacy policies

4. To determine factors affecting privacy and data protection in developing nations particularly Nigeria.

5. To determine the general knowledge and perception Nigerians have about e-commerce and its dangers, data protection and privacy by conducting surveys and interviews. In particular, testing the following three hypotheses (see Section 5.1):

    i. *Hypothesis one: The current views of privacy are focussed mainly on financial aspects and knowledge of other aspects of privacy protection is insufficient.*

    ii. *Hypothesis two: The public generally shows higher levels of trust in private bodies rather than in the government to protect their privacy interest.*

    iii. Hypothesis three: Many people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it.

6. To develop recommendations based on the findings to improve general awareness of the dangers of e-commerce, privacy and data protection.

7. To develop a programme and recommendations that will improve e-commerce privacy and data protection in developing nations using the results from previous studies conducted in the research.

8. To evaluate the effectiveness of the proposed framework by conducting surveys, pilot testing and interviewing experts.

1.6 Thesis Structure

Chapter 1 (Introduction) provides a general introduction for the thesis, and describes the background of the research. It also describes the key area of research by illustrating the statement of research problem, aims and objectives, research scope and the thesis structure.

Chapter 2 (the Literature review) starts with discussing the general dangers of e-commerce including privacy issues. Subsequently, the review describes two common data protection regulatory approaches and describes self-protection techniques as a method. It identifies previous research on understanding the websites' privacy practices. It concentrates on the literature on Internet security awareness in general to demonstrate the need of this research and to define the scope and vision of the research solution.

Chapter 3 (The Study Context- Nigeria) gives an overview of Nigeria. It presents the level of Internet penetration and the current data protection regulatory framework.

Chapter 4 (Research Methodology) describes the direction of the research path from the justification of research philosophy, approach, and strategy to the decision of the data collection methods used in the research to fulfil the research aim and objectives.

Chapter 5 (Nigerians' Perceptions of Personal Data Protection and Privacy) provides the analysis of the questionnaire and interviews conducted to determine the general perceptions of Internet privacy and data protection in Nigeria.

Chapter 6 (Analysis of Data protection and Privacy Practices in Nigeria) provides an analysis of Nigerian websites privacy practices through content analysis and cookie crawler to analyse their data collection practices.

Chapter 7 (Interpretation of Government and Self-Regulation Data Protection Approaches in Nigeria) evaluates the factors that determine the adoption of a privacy and data protection approach. It also evaluates data protection approaches to determine its applicability in developing countries.

Chapter 8 (Findings and recommendations) gathers the outcomes of the previous chapters to define a list of effective recommendations to help in reducing the privacy and data protection issue in Nigeria. The recommendations are directed to all target groups: the Nigerian government, Nigerian Internet users and private institutions responsible for ensuring Internet security.

Chapters 9 and 10 describes in detail the proposed awareness programme starting with the description of the proposed awareness programme in Chapter 8. Chapter 9 describes the development and evaluation of its effectiveness in enhancing awareness and reducing the privacy and data protection problem in Nigeria.

Finally, Chapter 11 (Conclusion and future work) presents a summary of the whole research outcome, including its limitations, and proposes recommendations for further studies.

Chapter 2 Literature Review

This chapter explores previous research in the area of e-commerce websites' privacy and data protection practices and Internet security awareness. It provides background knowledge on related topics and terms, such as how the perception of e-commerce data protection and privacy can influence privacy practice and awareness in a country. Furthermore, it explores various studies done on websites privacy practices and various Internet security awareness initiatives being adopted.

2.1 Dangers of E-commerce

Although e-commerce comes with numerous benefits, there can be problems if there is not full awareness of the risks. This section will briefly discuss some risks that come with Internet transactions.

2.1.1 Privacy in E-Commerce

Companies use e-commerce sites to reach potential customers. During the e-commerce process, most online businesses make use of customers' data to provide customised advertising and personalised services, building strategic relationships with customers. This benefits the customers as they have access to personalised programmes, loyalty benefit and so on. However, it can also be misused, for example, by sending unwanted emails to customers, selling customers' information to others, or disclosing potentially sensitive information that the customer would prefer to keep private (Dinev and Hart, 2006; Carr, 2010). The easiest way to gather personal information is during a registration or ordering process. Customers are asked for personal information such as name, email address, and credit card number. Some of these data are required to process transactions. However, additional information can also be

collected such as preferences, income, and other types of personal information that can help target marketing efforts (Carr, 2010). The third approach is to gather customers' personal information by the use of "cookies". These are files stored in an individual's computer that contain information such as the customer's traits, preferences, and behavioural information that can be accessed and used to identify the individual (Penenberg, 2005). With the introduction and popularity of social networks, a fourth approach has became available: harvesting personal information from social networks such as Facebook, Twitter, YouTube, and Flickr (Ingram, 2012). Many customers are concerned about their personal data being used inappropriately, which could reduce customers' trust in e-commerce (Sarathy and Robertson, 2003a).

2.1.2 Hacking

Hacking with the purpose of stealing confidential data is a very popular cyber-attack known today. Once a user's account is compromised, there could be ramifications such as identity theft. A hacker can gain access to very confidential information such as bank account and credit/debit card details, home address and so on. (Barber, 2001). Poorly coded or incorrectly configured websites are making it easy for hackers to attack sites and gain unsuspecting customers' information. The lack of user awareness also makes for a successful hacking (Parr, 2014). Some of the common ways hackers can gain access to information online are discussed in 2.1.2.1.

2.1.2.1 Session Hijacking/Cookie Hijacking

Session Hijacking is the exploitation of a valid computer session, sometimes also called a session key, to gain unauthorized access to information or services in a computer system (Khanna and Chaudhry, 2012). This is usually directed at e-commerce websites where users provide personal information for the purpose of a transaction (Barber, 2001). The HTTP

cookies, used to maintain a session on many web sites, can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. Some websites require users to be authenticated with a username and password to formally set up as session. Cookies are used as a form of session tracking to ensure the user is still logged in. Where network traffic is not encrypted, attackers can therefore read the communications of other users on the network, including cookies. Using this intercepted communication, an attacker can impersonate the user and gain access to the user's account, which will have very confidential data such as their credit/debit card details, address, date of birth, and so on. An attacker could use intercepted cookies to impersonate a user and perform a malicious task, such as transferring money out of the victim's bank account (Khanna and Chaudhry, 2012).

2.1.2.2 Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by setting up a replica of an original site (Ramzan, 2010; Khanna and Chaudhry, 2012). The hacker only requires a little knowledge of PHP, HTML, CSS, and DHTML. The hacker just needs to mimic the HTML code of the original website. The phisher deceives people by using similar e-mails to those mailed by well-known enterprises, for example banks. These e-mails often ask users to provide personal information, or result in users losing their personal rights; they usually contain a counterfeit URL which links to a website where the users can fill in the required information. People are often trapped by phishing due to inattention (Chen, Jeng and Liu, 2006). Hackers lure users by sending emails that contain alarming messages for example, "your account has been compromised" or "account will be disabled". Another method used is in the form of aid-seeking e-mails. These e-mails usually request their users to visit a link that seemingly links to some charitable

organization's website but, in truth, links the readers to a website that will install a Trojan program on the reader's computer (Khanna and Chaudhry, 2012; Chen, Jeng and Liu, 2006).

2.1.2.3 Cross-Sites Scripting

Cross-site scripting is a type of computer security vulnerability typically found in Web applications. Cross-site scripting enables attackers to inject malicious script into Web pages viewed by other users. The attacks occur when a hacker uses a web application to send malicious code, usually in the form of a browser-side script. The user's browser has no way to know that the script is malicious and will execute the script (Khanna and Chaudhry, 2012). The malicious script can access any cookies or personal information retained by the browser (Bradbury, 2012)

2.1.2.4 Cross-site Request Forgery

This is a type of malicious exploit of a website whereby unauthorised commands are transmitted from a user that the website trusts. Unlike cross-site scripting, which exploits the trust a user has for a particular site, cross-site request forgery exploits the trust that a site has in a user's browser (Bradbury, 2012). By luring the user by for example, sending a link via email or chat, the hacker can force the user to execute the hacker's bidding. Cross-site request forgery attacks capitalise on the fact that a user is already logged into a website. If the user's cookie is still valid and the user authenticated, the cross-site request forgery attack will work (Bradbury, 2012).

2.1.2.5 Direct Harvesting Attack

A directory harvesting attack is a means adopted by an attacker to identify the valid email addresses configured on a mail server. The attack is usually carried out by way of a standard dictionary attack, where valid e-mail addresses are found by instinctive force guessing valid

e-mail addresses at a domain using different permutations of common usernames (Khanna and Chaudhry, 2012). When successful, the addresses are sold to spammers who would want to use them for unacceptable purposes for example data theft.

2.1.2.6 Trojan Horse

A Trojan horse is a program that uses malicious code disguised as a trusted program. Once installed it ends up installing a virus, which usually has the ability to steal, record everything you type and send it back to the hacker. To deploy a Trojan, the hacker can send it to the victim as an attachment to an email and, once opened, the Trojan will drop into the victim's system (Khanna and Chaudhry, 2012). Certain Trojan programs are designed especially for instant messengers. Hackers use the instant communication capability to plant a Trojan program into an unsuspected program; the planted program is a kind of remotely controlled hacking tool that can disguise itself and is unauthorized. The Trojan program can read, delete, move and execute any file on the computer (Chen, Jeng and Liu, 2006).

2.1.2.7 Impersonation

There are various ways through which a hacker can impersonate other users. For instance, a hacker after stealing a user's information impersonates the victim. The victim's contacts not knowing that the account has been hacked believe that the person they're talking to is the victim, and are persuaded to execute certain requests or reveal confidential information (Chen, Jeng and Liu, 2006)

The risks described in Section 2.1.2 can be countered by a number of approaches, including regulation and privacy-enhancing technologies. These will be discussed further in Section 2.3.

2.2 Different Data Protection Regulatory Approaches (Government and Self-Regulated)

Due to concern about privacy issues, the Organization for Economic Cooperation and Development (OECD), the U.S. government, and the European Union began extensive discussions about developing a regulatory framework for privacy (Cate and Mayer-Schönberger, 2013). These discussions were guided by eight privacy principles: (1) Collection Limitation (2) Data Quality (3) Purpose Specification (4) Use Limitation (5) Security Safeguards (6) Openness (7) Individual Participation (8) Accountability

The United Kingdom decided to adopt the formal enforcement in the form of the Data Protection Act, 1998, incorporating the eight OECD principles while the United States, although endorsing the principles, adopted the self-regulation approach rather than governmental regulation (Jamal, Maier and Sunder, 2005a).

Understanding these differences in regulatory approaches is a key to successfully meeting information privacy requirements in developing nations.

2.2.1 Government Approach: Privacy Legislation in the United Kingdom

The United Kingdom is known for their particularly rigorous privacy laws. They have taken a firmer stance in order to provide strong legal protection of individual privacy rights. Directive 95/46/EC of the European Parliament and of the Council was issued on 24 October 1995. It deals with issues on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The UK Government was required to implement this Directive, which it did in the form of the Data Protection Act 1998. It came into force on 1 March 2000. This totally replaced the

Data Protection Act of 1984 (Information Resources Management Association, 2001) The Information commissioner, a British Government agency enforces the privacy law. Any website based in the United Kingdom that collects personal information are required by law to inform the Information Commissioner and abide by the eight principles of the data protection act (Jamal, Maier and Sunder, 2005b). The principles provide guidelines and specifications for collecting and processing personal data. In addition, all e-commerce websites are required to have a privacy policy that informs website visitors how the website will retain, process, disclose and remove their data in line with the principles (Legislation, 2016). In 2012, The European Commission's Directorate-General for Justice implemented a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy (MacDermott and Smith, 2013)

2.2.2 Self-Regulation Approach: Industry Self-Regulation in the United States

In the United States, data protection is left mostly to evolution of industry norms and voluntary compliance. Each company is responsible for deciding on the degree of information that is collected and used, and for developing its own privacy policy statement based on its industry guidelines (Boritz and No, 2011; Jamal, Maier and Sunder, 2005b). In addition, there are many guidelines, developed by governmental agencies and industry groups that are not legally enforceable but are part of self-regulatory efforts and are considered “best practices” (Jamal, Maier and Sunder, 2003). There is no legal requirement in the U.S. for commercial websites or online service providers to maintain privacy policies (Jamal, Maier and Sunder, 2005a). Due to the absence of and data protection legislation, US companies are adopting alternative means of assuring their customers of proper privacy practices (Jamal, Maier and Sunder, 2005a).

Third party organisations, for example TRUSTe, promote proper privacy practices and many U.S. Web sites display a Web seal to signal their compliance with the privacy standards formulated by the organisation. One of the conditions for receiving a web seal is the companies' implementation of Fair Information Practices (TRUSTe, 2017b).

The Fair Information Practices was issued in response to the growing use of automated data systems containing information about individuals. They usually stand as the standard for privacy recommendations (Antón, Earp and Reese, 2002). Since 1973, the Fair Information Practice (FIP) principles have served as the basis for establishing and evaluating U.S. privacy laws and practices (Federal Trade Commission, 2000). The FIP principles consist of: 1) notice/awareness; 2) choice/consent; 3) access/participation; 4) integrity/security; and 5) enforcement/redress. Government agencies, Internet users, and industry leaders all agree that privacy policies should reflect the FIPs (Gellman and Dixon, 2011). The Organisation for Economic Cooperation and Development (OECD), an international organization, issued the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013; Gellman, 2014). The U.S. FIPs do not include all of the OECD guidelines, but a subdivision. The FIP guidelines were incorporated in this research (Chapter 6) because the majority of websites in Nigeria are hosted in the United States and the FIP guidelines is the adopted industry guidelines in the U.S (Jamal, Maier and Sunder, 2005b)

2.2.3 Reliability of the Data Protection Approaches

A study by Jamal, Maier et al (2005) reports results of a comparative field study of two divergent approaches to regulating e-commerce privacy practices in United States and United Kingdom. The comparative study of the performance of these two regimes covers two dimensions of privacy, a choice/consent dimension and a notice/awareness dimension. They concluded that the U.S. Web sites that displayed the web seals performed at least as well as,

and on average better than, the U.K. Web sites in protecting the privacy of their users. The study revealed that privacy has fared no better in the United Kingdom than in the unregulated U.S. environment. It was also pointed out that, in the absence of mandated laws and requirements, U.S. Web sites tend to view the disclosure and adherence of privacy policies as part of their marketing strategy to attract consumers.

A paper by MacDermott and Smith (2013) points out that the great difference between the EU and US approaches presents significant problems for global interoperability and neither promises to result in practical and feasible consumer protection, at least not in the near term. They state that the European Union's government-centred approach raises serious questions of public and corporate costs, feasibility, and the prospect of cumbersome regulation inhibiting the overall growth of the Internet.

Although there may be pros and cons of adopting either data protection approach as the studies above have discussed, there are reasons to question whether either of these approaches can effectively address the Internet privacy problem independently. Additionally, another question to answer is if these regulations affect the online behaviour and awareness of Internet users and websites. Hirsch (2011) suggests co-regulation, in which government and industry share responsibility for drafting and enforcing regulatory standards. It is neither pure government regulation, nor pure self-regulation, but rather a mix of both.

A study by Park (2013) questions Internet policies provided by the FTC (Federal Trade Commission), which is grounded on the assumption of that Internet users are aware of and competent in exercising privacy control. He argues against this and indicates that the users are far from competent in exercising privacy control. This consequently could render these Internet policies less effective in protecting the privacy of Internet users. Birnhack and Elkin-Koren (2009) investigated the compliance of 1360 websites with legal requirements related to

information privacy. The findings show that only a small minority of websites comply with legal requirements.

Brookman (2015) discusses how that the sole adoption of just self-regulation and other legal protections are not effective enough to combat the increasing and persistent privacy issues and concerns. He argues that in the face of these inefficient data protection approaches, Internet users have the obligation to take affirmative measures to protect their own privacy.

One contribution of this study is analysing the effectiveness of both approaches, bringing important factors such as the awareness of Internet users and how privacy is perceived in a country into consideration. The study considers the effectiveness of protecting online privacy from not only the perspective of online retailers but also the perspective of the Internet users.

2.2.4 E-commerce and data protection in some developing nations

'Developing countries' is a term that refers to a broad range of countries that generally lack a high degree of industrialisation, infrastructure and other capital investment, sophisticated technology, widespread literacy and advanced living conditions (ASYCUDA, 2017). This section briefly explores data protection in some developing countries with a similar data protection approach to Nigeria.

2.2.4.1 Ghana

Ghana implements the government regulation data protection system. The Data Protection Act was passed in May 2012. This Act established a Data Protection Commission to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters (Fulbright, 2013). A bill was initially passed in 2009 for considerations but was withdrawn for amendment purposes (Acquaye, 2011). Data Controllers must apply for

registration (notification) on the Data Protection Register (DPR). On registration, data controllers must provide details of the data to be stored and its use, and the measures to be taken to comply with the Ac. The DPR is overseen by the Information Commissioner (Sampson, 2013).

2.2.4.2 India

There is little legislation in India which deals with the data protection, but there is the Personal Data Protection Bill which was introduced in the Parliament in 2006 but is yet to be passed (Kumaraguru and Sachdeva, 2012). The Information Technology Act, 2000 (IT Act), contains the provisions for the cyber and related IT laws in India. In the Information Technology Act, 2000 Act, Section 43A provides for protection of sensitive personal data and information of individuals (Ministry of Law, Justice and Company Affairs, 2000). A corporate body possessing, dealing with or handling sensitive personal data or information in a computer resource must implement and maintain reasonable security practices and procedures. If the body corporate is negligent in implementing these security practices and procedures and as a result causes wrongful loss or wrongful gain to any person, it may be required to pay damages to the affected person (Mathias and Kazia, 2016). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (IT Rules) which is framed under section 43A of the IT act set out the reasonable security practices and procedures that must be implemented to protect sensitive personal data (Ministry of Law, Justice and Company Affairs, 2000). The IT Rules define sensitive personal information as personal information relating to passwords, financial information such as bank account or credit card details, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information.

There are no national regulators dealing with enforcement of the Information Technology Act, 2000 Act. However, in cases where the compensation amount claimed for failure to protect confidentiality of sensitive personal information is less than INR50 million, the government appoints an adjudicating officer. The adjudicating officer has the power of a civil court, i.e. it can issue summons, take evidence on affidavits, and require discovery and production of documents (Mathias and Kazia, 2016).

2.2.4.3 Zimbabwe

Although there is no explicit constitutional 'right to privacy' in Zimbabwe, there is, however, various elements of the right to privacy that are found in different sections of the constitution (Fulbright, 2013). Zimbabwe has not yet defined privacy in the context of the protection of personal information, nor does the country's constitution provide explicit provisions for the protection of an individual's right to privacy (Ncube, 2004). Existing law only protects data held and used by the public sector. The Access to Information and Protection of Privacy indicates certain exceptions, restrictions on the use and disclosure of personal information by a number of public bodies, including professional associations, medical aid societies and public companies (Fulbright, 2013).

Most developing nations have no e-commerce data protection system or they are just in the process of enacting one (Akinsuyi, 2010). This is evident in the countries described in this section, whose data protection system is similar to that of Nigeria. Another similarity is the attempt to adopt full government regulation data protection approaches similar to that of developed countries.

One of the outcomes of this study is that relying on government regulation may not currently be an effective mitigation strategy for data protection and privacy. This is further discussed in Chapter 7 in the thesis.

2.3 Self-Protection Recommendations

Whenever Internet users make use of information services, they leave traces making it possible for anybody interested enough to collect, organise and analyse the personal data. This section introduces some recommendations given in the literature that users can use to prevent and reduce hacking and cyber-attacks, and enhance privacy, especially when performing transactions online.

2.3.1 Being Cautious of Public Wi-Fi and Computers

As convenient as free Wi-Fi and publicly available computers may be, using them can leave a user's personal information exposed (Mediati, 2011). Public computers might be infected with spyware and other types of malware devised to track movements online and collect passwords. Widely available freeware makes eavesdropping on emails and web browsing as simple as pressing a button (Mediati, 2011). Cyber attackers may also set up rogue Wi-Fi networks disguised as legitimate ones in order to steal personal information such as banking credentials, account passwords and so on. (Diallo, 2014). It is important to always verify that the network is legitimate before connection. The public network should not be used to check e-mails, use social network accounts, conduct online banking, or perform any other action that entails logging in to a site (Diallo, 2014). Using a VPN (Virtual Private Network), helps encrypt data that passes through a network. This can prevent cybercriminals from intercepting data (Mediati, 2011; Lipka, 2013).

2.3.2 Upgrade to the Latest Antivirus Software

Modern antivirus software can help protect from browser hijackers, Trojan horses, adware and spyware (Henry, 2013). Some products also include protection from other threats, such as infected and malicious URLs, spam, scam and phishing attacks, online banking attacks, and

social engineering techniques. Given how frequently new viruses are being created, the ability to protect against unknown malware is critical.

2.3.3 Use of Pseudonyms

The idea of pseudonyms is to hide the real identity of a user by using a bogus identity. Pseudonyms prevent service providers from linking an isolated transaction to a certain user (Langendörfer *et al.,* 2008). There will be minimal damage if a personal account is hacked, because the user is sure that there is no personal data in the account profile.

2.3.4 Hypertext Transfer Protocol Secure (HTTPS)

HTTPS encrypts the connection between the PC and the Website. Though HTTPS does not guarantee that a site is secure, it can help prevent other parties from hacking into the network and gaining access to a user's account (Mediati, 2011). HTTPS provides authentication of the website and associated web server that one is communicating with, which protect against hacking techniques like session or cookie hijacking. This provides a reasonable guarantee that the user is communicating with precisely the website that they intended to communicate with instead of an imposter as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party (Rouse, 2008). A user can tell if they are connected to a secure website if the website URL begins with https:// instead of http://.

2.3.5 Cookie Management

Another method for protecting a user's privacy is dealing with cookies. Although cookies are a very powerful technology for enhancing website interactivity, they can also be misused in ways that could be an abuse of personal privacy. Personal information is often stored in cookie files (passwords, credit card details), which passes openly over the Internet. The

contents of the cookie could be accessible to anybody capable of intercepting the cookie on the Internet (Session Hijacking) or maliciously gaining remote access to the user's computer (Seničar, Jerman-Blažič and Klobučar, 2003). The user has no control as to whether there are security measures being taken with cookie file transfer and storage. Although a user can manage cookies by

- Deleting cookies
- Selectively accepting cookie files
- Viewing cookie files

2.3.6 Anonymiser

An anonymiser or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between the users' computer and the rest of the Internet (Cottrell, 2014a). An account is created with a 'trusted' Internet Service Provider. A user can register their personal details with assurance that they will not be passed onto other parties or used for marketing purposes (Seničar, Jerman-Blažič and Klobučar, 2003)

2.3.7 Remailers

These are programs that accept mail, strip off information that would identify the origin of the message, and forward the mail to the designated recipient (Seničar, Jerman-Blažič and Klobučar, 2003; Cottrell, 2014b; Cottrell, 2014a).

2.3.8 Link Checker Plug-in

Legitimate sites may be hacked and cybercriminals use fake search engines to ensure that their infected pages come up in searches and seemingly safe sites may harbour malware (Mediati, 2011). Link-checker tools show small badges next to links in search results and elsewhere to indicate whether a site is trustworthy, dangerous, or questionable. The tools also add a status indicator to your browser's toolbar to signal the presence of any problems with the site that you are currently visiting (Mediati, 2011).

Although legislation and web seals try to ensure that websites and companies have adequate security and procedures in place to protect users, the users also have responsibility to ensure their own cyber safety in the case where organisations are breached or unable to provide adequate security (Kritzinger and von Solms, 2010).

2.4 Website Privacy Practices

The rise of the Internet has opened up new ways for people to obtain information, interact and do business with each other. E-commerce is one of the most important ways the Internet has brought about a digital revolution. Consumers can now research and compare products and make purchases from their home or workplace, obtaining far more information more quickly than they ever could before. The Internet has also reduced the costs of gathering, storing, manipulating and transmitting information of all kinds. Accordingly, concerns about the privacy of Internet users have grown in importance (Adkinson, Eisenach and Lenard, 2002)

Internet users are concerned about threats to their privacy when online. Several studies have shown, however, that Internet users are more inclined to trust a website if it simply posts a

privacy policy (Adkinson, Eisenach and Lenard, 2002; Meinert *et al.,* 2006). Most online companies now post privacy policies on their website, but not all consumers can or are willing to take the time to read and understand them. It is usually difficult to check if e-commerce websites do not deviate from the practices stated on their policy. One of the ways compliance of a website with privacy standards can be verified is by identifying how a website uses cookies to monitor activity and the presence of third party cookies (Jamal, Maier and Sunder, 2005c).

2.4.1 Prior Studies Examining Website Privacy Practice and/or Disclosure

Prior investigations of website privacy practices have been done to provide insight on the state of practice versus disclosure (Miyazaki, 2008).

Marotta-Wurgler (Marotta-Wurgler, 2016) reviewed the privacy policies of 261 websites by tracking the presence or absence of terms pertaining to notice, information collection and sharing, data security, and other practices and compare stated practices with various regulatory guidelines. The analysis revealed facts about current privacy practices, but the overall finding is that compliance with current guidelines seems low. In terms of substance, data collection and sharing is widespread and difficult for the user to control. In fact, data collection and sharing practices are not just hard to control, they are hard or simply impossible to learn.

Antón, Earp et al (2002) created a comprehensive taxonomy for privacy-related system goals so that consumers and system developers can more accurately compare a website's privacy practices functionality with its stated policies. They derived the taxonomy from the Fair Information Practices (FIPs) since it serves as the standard for privacy recommendations (Antón, Earp and Reese, 2002). The goals are subdivided according to the FIP categories (Landesberg *et al.,* 1998) as defined in table 2.1.

Table 2.1: Privacy goals and taxonomy classification

Protection Goal Taxonomy	Protection Goal Sub-Classifications
Notice/Awareness Goals asserting that consumers should be notified and/or made aware of an organization's information practices before any information is actually collected from them (for example, an organization's privacy policy).	• General Notice/Awareness • Identification of the Uses to Which the Data Will be Put • Identification of Any Potential Recipients of the Data • 3rd Party Limitations • Nature of the Data Collected • Steps Taken by the Data Collector to ensure the confidentiality, • Integrity, and Quality of the Data
Choice/Consent Goals ensuring that consumers are given the option to decide what personal information collected about them is to be used and whether it may be used for secondary purposes.	• Choice of How Data is Used • Choice of Sharing Data • Choice of What Data is Taken/Stored
Access/Participation Goals allowing or restricting access to a particular site or functionality based on whether or not the consumer provides their PII. Goals in this category address also the ability for consumers to access or correct any personally identifiable information about them.	• PII Provision Required • PII Provision Optional • Providing consumer access to data

Integrity/Security Goals ensuring that data is both accurate and secure. Security and accuracy comes from both the consumer and the organization collecting the PII. Goals in this category range from vague statements stating only that PII is kept securely to specific technical goals of what security protocols will be used to transfer PII over the Internet	• Mission Statement • User-Supplied Integrity Goals • Using Anonymous PII • Destroying Untimely or Sensitive Data • Managerial Measures to Protect Against Loss and the Unauthorized • Access, Destruction, Use, or Disclosure of the Data • Technical Measures to Protect Against Loss and the unauthorised access, destruction, use, or disclosure of the data
Enforcement/Redress Goals addressing the mechanisms that are in place to enforce privacy, otherwise a policy is merely suggestive, rather than prescriptive. Prescribe a way of working and general guidelines companies should follow. These include both self-imposed and government imposed work restrictions.	• Operational Prevention Assurance • 3rd Party Prevention Assurance

If the goal is to make privacy protection more effective and efficient, it is important to know if a website has policies and if they follow the policies. However, it is difficult to find this out. Although e-commerce is still developing in Nigeria, it is important to emphasise the need for websites to adopt good practices without deviating from stated practices.

2.4.2 Perceptions of Personal Data Protection and Privacy

Many academic research and press articles about Internet users' privacy concerns are being published (Klien, 2004; Hong and Thong, 2013; Taddicken, 2014; Bergström, 2015). However, the understanding and perception of privacy is changeable and relative.

Privacy perceptions from the developed world may not be applicable to the developing world due to unique situations in developing regions (Kumaraguru and Sachdeva, 2014). These unique situations could include, economic situations, literacy, reliability of the government and lack of privacy laws. Studies have shown that perception of privacy differs from country to country (Sarathy and Robertson, 2003b). The differences in privacy perception could affect their awareness on Internet security and its general privacy practices. Several studies have shown that users' overall security perception is shaped by their awareness of security threats and available countermeasures (Ifinedo, 2012; Huang *et al.,* 2011; Furnell, Bryant and Phippen, 2007). Internet security awareness and a lack of knowledge of how to implement the available security measures could be a hindrance to the safe adoption of e-commerce.

The Eurobarometer survey conducted in 2015, asked 28,000 EU citizens what they think about the protection of their personal data (Eurobarometer, 2015). More specifically, the report addresses Europeans' actual disclosure of personal information, their awareness of and perceived control over their personal data, their ways of protecting personal data, and the data protection regulation they would like to see. The Eurobarometer survey found that nine out of ten Europeans thought that it is important for them to have the same rights and protection over their personal information, regardless of the country in which the public authority or private company offering the service is based. Over four out of ten respondents thought the enforcement of rules on personal data protection should be handled at European level. The report also demonstrates that Europeans have widespread concerns about the consequences of their data being misused. More than two thirds of respondents who stated that they do not have complete control over their personal data say they are concerned about this lack of control. In general, although the majority of Europeans have accepted the disclosure of personal information as fact of modern life, they appear to be quite concerned about their privacy. Considerable proportions of Europeans appear to be in need of information on what

constitutes personal data.

A research study was conducted to examine Americans' privacy perceptions (Madden *et al.,* 2014). The study discovered that most of the American population lack confidence that they have control over their personal information. Unlike European citizens, few Americans thought that the government and corporations can be trusted with their personal information. They also had the opinion that the government could do more to regulate what advertisers do with their personal information. In addition, when it comes to their own role in managing the personal information they consider sensitive, most adults express a desire to have more information on additional steps to protect their data online. The study also found that social security numbers are considered to be the most sensitive piece of personal information, while media tastes and purchasing habits are considered among the least sensitive categories of data.

Another study focused on the privacy perceptions of Indian citizens (Kumaraguru and Sachdeva, 2012). Data was collected from 10,427 survey respondents. The study found out that citizens have misinformed mental models of the privacy situation; for instance some of the participants (49%) felt that there is a law which protects them whereas there is no privacy law in India. There is also a general reduction in the trust in the government. Most participants felt passwords to be the most protected Personally Identifiable Information (PII) and then, financial information (bank, credit card details). Participants were aware of privacy issues related to financial data, thanks to various publicised financial frauds and thefts that has created the awareness. Many of the participants had never read the privacy policy on any website that they had interacted with before sharing their personal information.

Section 2.5 looks at awareness as a possible solution to Internet security and discusses other studies that have investigated various approaches to security awareness

2.5 E-commerce and Internet Security Awareness

Internet Security awareness must be effective and should address all ages, including both workplace and domestic environments. It is also important to ensure that Internet security is well conveyed and all relevant audiences receive adequate attention (Rahim *et al.,* 2015). Internet security awareness is briefly defined as a methodology to educate Internet users to be sensitive to the various cyber threats and the vulnerability of computers and data to these threats (Siponen, 2000). Internet security awareness can also be defined as the degree of users' understanding about the importance of information security, and their responsibilities to exercise sufficient levels of information control to protect their data (Shaw *et al.,* 2009).

Information is very important as far as e-commerce is concerned and the protection of information is crucial in this digital age. Internet users must navigate a wide range of risks to their privacy and their systems' security. Typical users are often unaware of or misunderstand these risks and are ill equipped to use available tools to manage them. Awareness issues are usually identified as one of the key triggers to poor cyber-security culture (Woon, Tan and Low, 2005; Flinn and Lumsden, 2005; Gcaza and von Solms, 2017; Reid and Van Niekerk, 2014).

A study discovered that experienced Internet users perceived threats such as hackers, worms and viruses as dangerous, however threats such as spam are perceived as lower risk (Huang, Rau and Salvendy, 2010). It was discovered that the level of awareness of likelihood, severity and knowledge of threats influences overall perception. This finding was corroborated with a similar study (Kanich *et al.,* 2008). Although spam can be responsible for the spread of malware, such as viruses, it was rated as a lower threat to malware such as viruses.

Another experiment by Huang, Rau et al (2011) investigated if security perceptions can be adjusted to improve intentions to adopt security measures. Their experiment involved two

groups of participants, where one group received security information about e-banking security threats. The group had higher perceptions of security threats and was more likely to adopt e-banking security measures. The results indicated that people are more likely to adopt self-protection techniques if the applicable knowledge and awareness is provided.

Awareness of current cyber-security technologies is especially important because it plays a significant role in shaping how users perceived the available security measures (Dhamija, Tygar and Hearst, 2006; Dinev and Hu, 2007). An analysis conducted on phishing attacks, found that users who lack basic knowledge of browser features are more likely to ignore security indicators such as HTTPS, which lead to successful phishing attacks (Dhamija, Tygar and Hearst, 2006). A different study suggested a compulsory e-awareness portal for Internet users before they go online. They point out that although research has been done on making users aware of the importance of securing their own information, the enforcement to do so does not usually exist (Kritzinger and von Solms, 2010). Therefore, many users venture onto the Internet without any idea of what the risks are and how they should protect themselves. Kritzinger and von Solms report that trusted legitimate websites are the perfect vehicle for malware distribution. With growing numbers of users accessing the Internet for many reasons, the big problem and worry is that, in many cases, such users are not information security aware, and are therefore potentially exposing themselves in a big way.

Internet security is highly dependent on educated users who are aware of and routinely employ sound practices. Unfortunately, most customers believe that security is solely the responsibility of a third party, for instance, the government, website, banks, or IT professionals (John, 2004). To combat this problem, it is necessary to conduct an awareness and outreach programme. In order for the programme to be effective, it is necessary to first understand users' perceptions of privacy and data protection. Awareness efforts are needed to attract people's attention to get them interested in privacy and security measures. This is to

reinforce good security practices by allowing individuals to recognise privacy concerns and respond accordingly. The future of electronic commerce depends on enhancing consumers' security perceptions and maintaining the balance between perceived trust and online security.

2.5.1 Internet Security Awareness Training

Internet security awareness is a proactive measure that has to do with making Internet users aware of how to protect their personal information. As previously discussed in Section 2.5, Internet security awareness is associated with users' perceptions and behaviour, ultimately it is important to modify users' perceptions to improve Internet security. To improve Internet security practices, awareness of Internet security issues and measures is important, and one approach is to provide security awareness training. An awareness programme should be developed with the following in mind (Furman *et al.,* 2011)

- What behaviour should be reinforced?
- What skills should the users learn and apply?

It is also very important to make an awareness programme interesting, attractive and current in order to attract users' attention. Effective user awareness training should enhance privacy and data protection knowledge while holding a trainee's attention sufficiently long enough to impart a message (Garcia, 2013). The aim of an awareness programme should be to cause change in (Tsohou *et al.,* 2008):

- Audience's perceptions
- Audience's familiarity with security policies and procedures and,
- Audience's interests towards Internet security.

2.5.2 Type of Internet Users

Internet users can be divided into two types (Kritzinger and von Solms, 2010), as described in Sections 2.5.2.1 and 2.5.2.2:

2.5.2.1 Non Home Users (NHU)

These are those users accessing the Internet from their corporate workstations within their work environments. Such users will come from the industry, government, academia and so on. NHUs are most probably exposed to compulsory information security awareness courses and will be governed by corporate policies, procedures, guidelines and best practices to complete such awareness courses and perform secure practices when accessing the Internet.

2.5.2.2 Home Users (HU)

These are citizens of any age and technical knowledge who accesses the Internet for personal use anywhere outside their work environments (Kritzinger and von Solms, 2010). Unlike Non-home users who have access to regular awareness training, home users have no enforcement to ensure that they obtain Internet security awareness knowledge and implement it. Evidence reveals that it is this group of users that are most at risk, with most of cyber-attacks being focused on them (Talib, Clarke and Furnell, 2010; Furnell, Bryant and Phippen, 2007). According to Kritzinger and von Solms (2010), one of the main reasons for this lack of information security awareness by HUs, is the fact that there is no enforcement by a third party to ensure that HUs are securely using the Internet or that their information security awareness is up to date.

Considering the definition of both home users and non-home users, freelance workers would fall under the category of home users since they are not exposed to compulsory awareness materials within a work environment.

2.5.3 Common Training and Awareness Techniques

Training and awareness is generally accomplished using one or a combination of several techniques described in this section (Cone *et al.,* 2007).

2.5.3.1 Formal Training Sessions

They can be instructor-led, seminars, or video sessions. “Formal” represents the traditional approach to user training and awareness. The success of this approach depends upon the ability of the training facilitator to engage the audience.

2.5.3.2 Passive Computer-based and Web-based Training

This represents a centralized approach to the training and awareness problem. It could be passive computer based. An example is the website “Be Cyber Street wise” (HM Government, 2015) whose aim is to measurably and significantly improve the online safety behaviour and confidence of consumers and small businesses or Interactive computer-based training, such as video games.

2.5.3.3 Strategic Placement of Awareness Messages

Strategic placement of awareness messages seek to raise the level of consciousness through the delivery of messages by methods such as posters in public places, email messages, and media advertising (TV adverts, newspapers, websites).

2.5.3.4 Contextual Training

Contextual training in the context of Internet security awareness, would aim to provide awareness training materials based on the current cyber threat. This ensures that both information and knowledge are context specific and in relation to the current risk (Nonaka and Takeuchi, 1995). Some researchers who have carried out such studies involving

contextual training have shown that any educational materials given to participants improved their knowledge on the threats and protection level (Jagatic *et al.,* 2007; Ferguson, 2005; Kumaraguru *et al.,* 2010).

2.5.4 Existing Information Security Awareness Approaches

Kureva, Loock and Kritzinger (2014) propose an Internet service provider-information security awareness framework (ISP-ISA). The ISP-ISA advances the involvement of relevant authorities such as Internet Service Providers (ISPs) to support Internet users with information security awareness. The proposed framework can influence the Internet users' behaviour to information security by presenting the relevant best practises in the form of a checklist. This ISP-ISA proposed that the responsibility be on the ISPs as they are the only point of contact between the Internet users and the Internet.

(Cone *et al.,* 2007) designed CyberCIEGE, which is described as a flexible, highly interactive video game, a security awareness tool that can support security-training objectives while engaging typical users in an engaging security adventure. This contrasts with many other forms of training, which can fail because they are rote and do not require users to think about and apply security concepts.

Mellor and Noyes (2007) also raise the issue of personal commitment and accountability in security training. Individual accountability represents taking ownership of something and understanding the consequences. When this is added to a training programme, it transforms the trainee from a passive learner to an active learner as they become individually accountable for the material presented. A baseline training and assessment instrument is created to cover ten domains of information security (proposed as: passwords, social engineering, email, physical security, locking or logging off your computer, unauthorized programs, handling confidential data and material, internet usage, phishing, and handling

storage media and portable computers). It consists of five phases according to the NIST SP800-16 proposal (needs analysis, goal formation design, development, implementation and evaluation). The study showed that a great deal of personal learning has occurred as individuals were personally instructed in each of the ten information security domains.

Abawajy's (2014) study suggests that security awareness training is a powerful means of empowering Internet users with knowledge on focused topics. Although the findings suggest that video presentation is the most preferred security awareness training delivery method, the training provided through the use of the various delivery methods appeared to have been mostly successful in providing more understanding of what phishing is and how to best minimise its dangers. This suggests that combined delivery methods are more effective than individual security awareness delivery method.

Hendrix, Al-Sherbaz and Victoria (2016) investigated whether games can be effective cyber security training tools. It was concluded that while it is challenging to answer generically whether games are effective cyber security training tools maybe the focus should be more on the type of scenario-based training that is already common in the security field, which often includes gaming elements. Games could then represent specific case studies and facilitate a case-based learning approach. The studies discussed perceive information security from a social perspective, when the focus is mainly on the human aspects of information security, and sociotechnical perspective, when the focus is rather balanced between the human interface and the technical aspects of security.

In addition to the studies mentioned, there are numerous websites that can be identified as valuable resources for raising the Internet security awareness level. Some representative websites are described below. The SANS Institute website (SANS, 2014) provides a dedicated section called "Securing the Human" in recognition of the need for training on

awareness and compliance for non-technical users. The objective of the site is to provide training and testing tools in order to ensure that security compliance requirements are met and, at the same time, a change in human behaviour is achieved. A variety of resources are available in various formats (for example training videos, awareness posters, screensavers, and so on.) and for different types of audiences like end users, developers, engineers, healthcare professionals and people working at utility organizations and so on. Area coverage is broad and includes the most common topics like social engineering, email and messaging, social networks, data security, use of Wi-Fi, use of passwords, and so on. The computer-based training approach allows participants to take training at their own pace from any location, in the form of 3-minute videos and accompanying them with support materials. This passive presentation of the awareness contents does not guarantee coverage or retention of topic knowledge. Figure 2.1 shows the training topics.

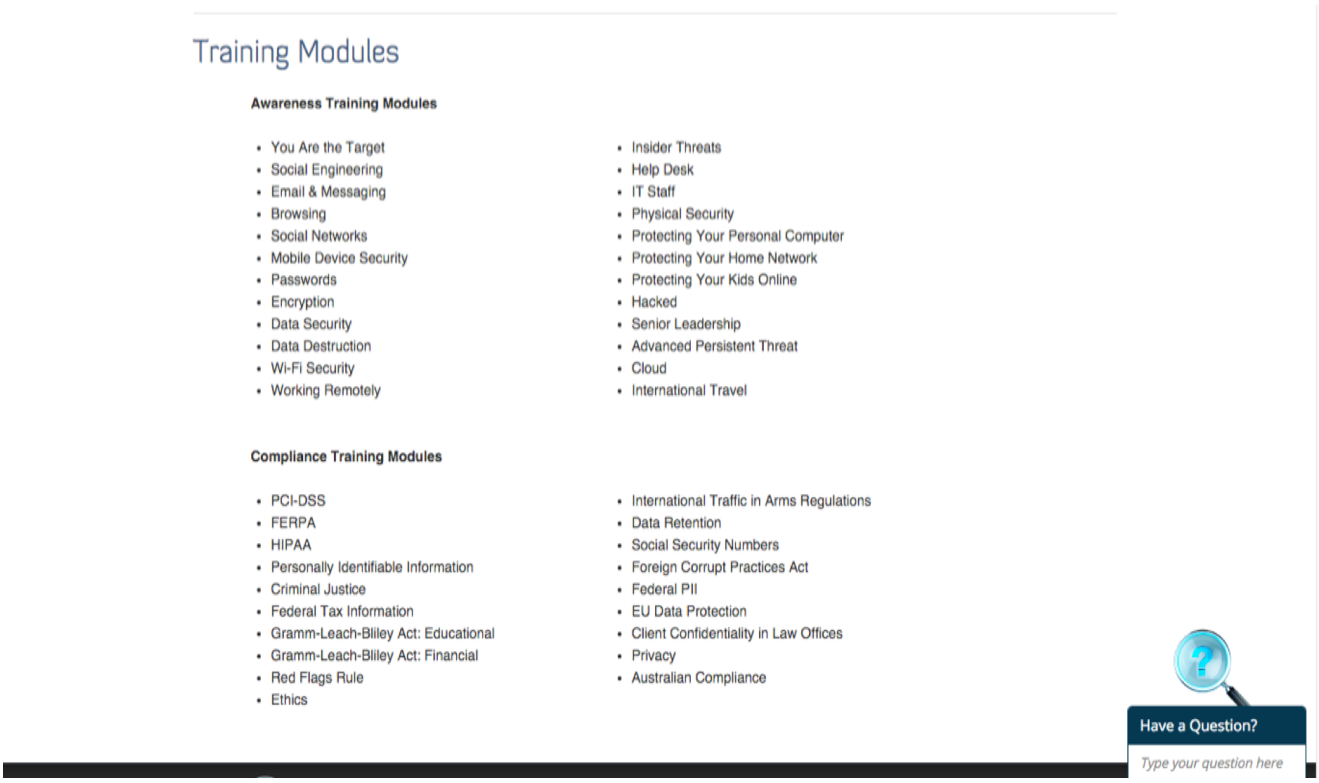

Figure 2.1: SANS security awareness training topics

Wired Safety (2014) contains security resources provided by volunteers among different age groups and different personalities (for example teachers, TV personalities, executives, writers and PhDs.) and is generally addressed to teenagers and their parents. Most of these resources are provided free of charge and visitors are able to find resources on the following major areas:

- Help and support for victims of cybercrime and harassment.
- Advice, training and help for law enforcement worldwide on preventing, spotting and investigating cybercrimes.
- Education for children, parents, communities, law enforcement and educators.
- Information and awareness on all aspects of online safety, privacy, responsible use and security.

- Resources that can be downloaded or printed and used for offline presentations, community events and classroom activities.

Main subjects include topics like privacy, safety, security and child protection. Some topics discussed, for example, distracted driving, which although serious issues, these are not related to Internet security awareness and efforts to change security culture.

A website, Stay Safe Online (NCSA, 2015) provides information on how to be safe when online and gives the opportunity to the public to take part in awareness initiatives such as the information security awareness month, celebrated every year during October. The website provides free resources such as posters, banners, security videos and so on. The topics are divided into the following categories:

- Information for home Internet users with topics about how to keep a machine clean, protect personal information, work with mobile devices, information specifically for parents and so on.

- Information for people responsible to teach online safety categorized into different age groups (for example middle & high school, higher education).

- Information for people already in a working environment that want to find information on how to protect their businesses for example SMEs

The Stop Think Connect (Stopthinkconnect, 2014) website represents a global effort aimed at increasing the understanding of cyber threats and empowering the public to be safer and more secure online. The site explains how average Internet users can protect themselves and their families against fraud, identity theft and other online threats. Information is presented in the form of various resources such as:

- Tip sheets, which contain brief text-based information on how to be protected at

various information security topics (for example mobile devices, privacy, games, social networking, and so on.). Some of them are addressed to specific age groups such as teens and parents.

- Posters ready to be used in order to raise awareness levels at specific topics.
- An online quiz that can be used to test the participant's knowledge on online safety, security and ethics. It contains 26 questions which are divided into two areas: (1) safety and security and (2) privacy and being a good online citizen.
- Memes on specific security topics (for example email safety, Wi-Fi usage and shopping online.), in an effort to mimic an information security topic in a humorous and easily transmitted way.
- Videos on a wide range of information security issues.

The websites described are typical examples of efforts towards raising the information security awareness level. They provide a wealth of information addressed to different population groups. However, most resources do not offer the ability to test a person's current knowledge or the knowledge acquired by using the web resources. In many instances, such testing and knowledge verification is desirable before being faced with the task of applying security precautions in a real world situation (Furnell, Gennatou and Dowland, 2002). All of the above validate the need for a more structured approach that could combine all these resources in a more efficient way.

2.6 Conclusion

The studies discussed in Section 2.2 show different perceptions of privacy from different nations. In some ways, this perception has encouraged different approaches in addressing the

privacy issues in the countries, especially in developed nations in Europe and North America. For instance, due to the relatively high level of trust in the government to handle privacy issues, the EU government regulates most of the privacy procedures as well as organises privacy awareness campaigns (Steinke 2002). Insights into the Nigerian perception of privacy issues can help develop regulation and tailor it to the specific needs and vulnerabilities with respect to personal data protection. It is particularly important to investigate ways to improve these perceptions. In order to raise the level of concern for security, an appropriate level of awareness must also be reached.

From the study of numerous articles discussed in 2.5, the importance of information security awareness and training in order to improve Internet security is clear. It was highlighted that security awareness is aimed at improving human security behaviour and, if human behaviour is improved, security awareness is also improved. It is evident that good solutions must be in place for secure information systems but without taking into consideration the human element, technical solutions will fail. Many researchers (Siponen, 2000; Mellor and Noyes, 2007; Cox, Connolly and Currall, 2001; Anttila *et al.,* 2007) highlight the importance and the effectiveness of improving user awareness on threats in reducing the risks, especially since technological solutions could be unreliable in providing full protection.

Accessing the web has many risks possibly with dire consequences for the user who has limited Internet privacy and security knowledge. It is beneficial for any awareness programme to be based on the Internet security requirements of the intended audience. It also is important for the programme to be easy to access, user-friendly, comprehensive, covering relevant topics, up to date and monitored for effectiveness. A combination of different training methods could be the best way of achieving this. Therefore, this research seeks to provide a solution to the e-commerce privacy and data protection issue in Nigeria by first determining the current issues in relation to applicable stakeholders and gaps to be filled and,

secondly, proposing effective recommendations for the stakeholders, which include an adapted awareness delivery method.

Chapter 3 provides an overview of the study context, Nigeria.

Chapter 3: The Study Context - Nigeria

This chapter begins by presenting an overview of Nigeria. It also briefly discusses the background to the research, specifically presenting the geographic context in which the study was conducted. Furthermore, the chapter describes the level of e-commerce and Internet penetration in Nigeria and gives an overview of the data protection regulatory framework.

3.1 Overview of Nigeria

According to the CIA world fact book (CIA, 2015), the Federal Republic of Nigeria, commonly referred to as Nigeria, is a federal constitutional republic in West Africa, bordering Benin in the west, Chad and Cameroon in the east, and Niger in the north. Its coast in the south lies on the Gulf of Guinea in the Atlantic Ocean. Nigeria consists of 36 States plus a Federal Capital Territory located in Abuja and is known to have over 274 ethnic groups in the Federation, which is divided into three major regions and grouped under six geopolitical zones with a total of 774 Local Government Areas. The official language is English and over 500 indigenous languages. It has an estimated population of over 183.5 million and the most populous country in the entire African Continent. It also has the 7th highest population in the world. Lagos is the commercial capital of the nation with an estimated population of 21 million, making Lagos the largest city in Africa.

Nigeria is a middle income, mixed economy and emerging market, with expanding financial, service, communications and technology and entertainment sectors. It is ranked 26th in the world in terms of GDP, and is the largest economy in Africa based on figures announced in April 2014. It is also on track to become one of the 20 largest economies in the world by 2020 (The Economist, 2014). Despite this sudden economic growth, Nigeria is still striving to

provide the basic infrastructure of a steady supply of electricity, good roads and transportation, health, education services and postal and telecommunication networks.

Figure 3.1: Geographical Context of the study (Central Intelligence Agency (CIA), 2017)

3.2 E-commerce and Internet Penetration

Internet penetration in Africa has greatly increased over the last half decade, but it is still lower than the world's average, however the continent seeks to close the ICT gap with the western world. According to Internet Live Stats (Internet Live Stats, 2017a), 28% of the continent had Internet access compared to 54% in the rest of the world.

Nigeria is ranked 10th on the list of the world's top Internet users and is first in Africa. According to Internet Live Stats, as of June 2011, there were 46.5 million Internet users

comprising 28.4% of the country's population, as indicated in Table 3.1. As of June 2016, there are approximately 86.2 million users comprising 46.1% of the country's population. The current development shows that in the last few years, computer access and Internet penetration has increasingly grown and this indicates a brighter future for Internet users in Nigeria.

Due to this growth in Internet usage, there has been increased visibility, activity and sales on popular Nigerian shopping websites, for example Konga.com and Jumia.com.ng. Moreover, online shops and merchants have exponentially increased within this short time, starting with only two online shops in 2004, the country boasted of over 75 as being active online by 2014 (Chiejina and Olamide, 2014).

Although there is great increase in e-commerce and Internet usage in Nigeria, there is still no effective data protection structure compared with developed nations, for example the United Kingdom. With the prevalent cybercrime and unskilled Internet users, there could be a significant risk to the state of Internet security in the country.

Table 3.2: Internet penetration in Nigeria (Internet Live Stats, 2017b)

Years	Users	% Penetration
2016	86.2 million	46.1
2014	75.7 million	42.7
2011	46.5 million	28.4

3.3 Nigerian Data Protection Regulatory Framework

The Nigerian Constitution recognises the right of privacy. However, Nigeria has not yet legislated any specific data protection law. A draft on guidelines on a Data Protection Bill, which was published by National Information Technology Development Agency (NITDA), was introduced in 2013 but it has not been passed as a law and there is no establishment of an institutional framework (Obutte, 2014). Another attempt to develop privacy protection was the passage of the Electronic Transaction Bill in 2015 by the 7th National Assembly, which contains data protection provisions of general application, but does not offer comprehensive data protection when compared with the United Kingdom Data Protection Act of 1998.

Regrettably, Nigeria does not have specific or comprehensive data protection legislation, comparable to other countries like the United Kingdom, Canada, and the United States of America, despite the repeated calls by industry stakeholders for its enactment (Perchstone & Graeys, 2016).

3.4 Conclusion

This chapter discussed the geographic context of Nigeria as a developing country with the largest population in the African continent. The chapter further considers the level of Internet penetration in Nigeria, which is regarded as being very low when compared to developed countries, despite Nigeria's remarkable increase in Internet usage. Finally, the Nigerian Data Protection Regulatory Framework, which provides a context of the data protection approach being adopted in Nigeria was discussed. This chapter has provided an introduction and overview of the study context. Chapter 4 discusses the methodology used in this study.

Chapter 4 Research Methodology

The purpose of this chapter is to describe the methodological approach that underpinned the research and contributed to achieving the objectives discussed in Section 1.5. It presents an overview of the research philosophy, strategy and provides a detailed description of the data collection methods used.

4.1 Research Philosophy

Research philosophy provides the context in which the relationships between data and research methods can be explored and analysed (Collis and Hussey, 2003). The research philosophy is influenced by the manner in which a researcher reasons about the development of knowledge and will affect the way the researcher conducts the research itself (Saunders and Lewis, 2009).

Positivism and Interpretivism are the two most recognised research philosophies, which may lead to the selection of the research design and methods (Orlikowski and Baroudi, 1991). The positivist approach maintains that a true explanation or cause of an event or social pattern can be found and tested by scientific observation and experimentation (Roth and Mehta, 2002; Myers, 1997). Positivists believe that by applying a similar process and carefully using statistical tests in investigating a large sample, different researchers observing the same factual problem will generate a similar result (Creswell, 2013).

The positivist research philosophy is commonly related to deduction and quantitative research methods, for example, surveys, experiments and field studies (Altinay, Paraskevas and Jang, 2015).

Interpretivism is mainly used by social scientists to study human behaviour, thus it is also referred to as social constructivism (Saunders and Lewis, 2009). According to Bryman (2015), interpretivists seek to understand human behaviour and the social world whereas a positivist would seek to explain the situation. In contrast to positivism, it generalises the findings and allows the researcher to interpret the data and gain an understanding of the context and process of the situation (Bryman, 2006).

According to Interpretivism, individuals with their own diverse backgrounds, assumptions and experiences contribute to the on-going construction of reality existing in their broader social context through social interaction (Wahyuni, 2012). Qualitative research, for example observations and interviews, is commonly related to the interpretive research philosophy (Altinay, Paraskevas and Jang, 2015).

Mixed methods research is an approach to knowledge that attempts to consider multiple viewpoints, perspectives, positions that always includes the perspectives of qualitative and quantitative research (Johnson, Onwuegbuzie and Turner, 2007).

With the rapid development of a new and complex information technologies, there are new challenges related to the understanding of IT capabilities, practices, usage, and impacts. As a result of these rapid changes, researchers often encounter situations in which existing theories and findings do not sufficiently explain or offer significant insights into a phenomenon of interest (Venkatesh, Brown and Bala, 2013).

A mixed methods approach was used in this research, combining qualitative and quantitative data to fully understand the phenomenon which was investigated. From this research perspective, the positivism approach is needed to collect the appropriate measurable and objective quantitative data to investigate and analyse Nigerian Internet users' perceptions of Internet privacy. This was achieved through designing a quantitative survey for Nigerian

Internet users. In addition, interpretivism is needed in this research to provide in-depth data and information regarding Nigerian Internet users' perceptions, understandings and attitudes towards privacy. It explores privacy issues not included in the quantitative survey and provides evidence explaining the main outcomes of the quantitative survey. Content analysis was also used to analyse Nigerian websites' privacy policies and data collection practices.

4.2 Research Strategy

The research strategy presents the major direction of the research and constitutes one of the important decisions made by the researcher (Pathirage, Amaratunga and Haigh, 2008). The choice of an appropriate research strategy not only reflects the nature of the study but the research objectives as well. Marshall and Rossman (2014) state that a research strategy consists of the overall rationale, the researcher's role, data collection methods, data management, data analysis strategy, trustworthiness features, and a management plan. There is a wide range of methods for conducting research such as experiments, action research, ethnography, case study, grounded theory and so on (Darke, Shanks and Broadbent, 1998; Leedy and Ormrod, 2005; Saunders and Lewis, 2009; Miles, Huberman and Saldana, 2013). Two research strategies (survey and case study) were adopted in this research.

4.2.1 Survey

A survey strategy provides a quantitative description of trends, attitudes or opinions of a population by studying a sample of that population (Creswell, 2013).

Researchers using this strategy assume that there are patterns that exist; however, surveys cannot confirm cause and effect in the same way as a scientific experiment but do give an

opportunity to see if an association exists between variables (Oates, 2005). Surveys do not always use questionnaires but can use interviews, observation or documentation.

The survey strategy is suitable for this research mainly due to the nature of the research and objectives and the need to understand and generate a general understanding of how privacy is perceived in Nigeria to help develop a framework and strategy for privacy in Nigeria. Questionnaires and Interviews were the approaches used in this research to collect data and information.

4.2.2 Case Study

Case study research is the study and analysis of a single or collective case, intended to capture the particularity and complexity of the object of study (Stake, 1995).

Case studies can be useful for exploring new or emerging processes or behaviours (Cassell and Symon, 2004; Ghauri and Grønhaug, 2005). Case studies have an important function in generating hypotheses and developing theory. The appropriate research strategy for this thesis is based on a case study of the phenomena of privacy and data protection in Nigeria**.**

The research employed an exploratory case study as it can be used where there is little in the literature about a topic in a specific context (i.e. Nigeria) (Yin, 2013). This type of study allows a researcher to gain more information about the topic, which people may know little about and can provide a platform upon which a further research project can be built (Oates, 2005).

One of the main disadvantages of adopting a case study approach is that it demonstrates very little about the generalisation of the main research findings. It is not certain that the main outcomes of the research are appropriate and useful elsewhere. However, the case study does

add to the body of evidence for the world as a whole and this study has shown that the recommendations can be of value in Nigeria.

4.3 Research Methods: Data Collection Techniques

In order to achieve the research aims, it is essential to obtain sufficient and relevant data through appropriate research methods.

Many researchers have used several research tools in their studies, in order to cross correlate their results and enhance the reliability and validity of them. People's information behaviour is a multidimensional procedure, which involves several characteristics. For this reason, it is important to use various research methods in order to capture as much information as possible (Byström, 1999; Wang, Hawk and Tenopir, 2000; Du and Spink, 2011). Based on the previously mentioned research philosophies, this research seeks to use a mixed-method approach for its design, which incorporates elements of both qualitative and quantitative research. This provides a better approach and allows for a detailed understanding of the research topic. The research methods used are a quantitative method through questionnaires with close-ended questions and then a qualitative method was applied through semi-structured interviews and finally content analysis in order to identify and allow a detailed understanding of the research topic.

4.3.1 Questionnaires

The questionnaires aimed to profile Nigerian Internet users' awareness and perception of privacy and data protection and also their knowledge of self-protection techniques. The questionnaires were distributed using different means, the self-administered method (paper based) and online. The questionnaire consists of a set of questions that reflects the main

topics of the research. This approach ensures that each participant reads and answers the same set of questions. This helps and ensures consistency and precision in the wording of the questions (Denscombe, 2003). The majority of the questions are closed and structured questions. This was required to allow only answers which fit the main research objectives (Denscombe, 2003). These questions allow the respondents to select an answer from a range of options. The Questionnaire was developed and designed using Qualtrics© software.

4.3.1.1 Questionnaire Design

The questionnaire included a covering letter as an introduction to the respondent. (See Appendix A2). This was needed to give the respondent a briefing of the research aim and objectives and to make respondents aware of the author's guarantee of the confidentiality of the responses.

To keep the questionnaire form short, only those items crucial to the research objectives were included. Hence, key items focused on individual perceptions about institutions that collect and use personal information and general perceptions of personal information. The sections in the questionnaires are as follows:

- **Personal Details**

  This section covered the respondents' gender, age and educational qualifications.

- **Perception of personal Information**

  This section examined Nigerians' disclosure of personal information, what they consider personal information to be and how they feel about disclosing their personal information online. This was to understand the perception of Internet privacy.

- **Perception of Personal Information Protection**

This section asked questions to determine the respondents' opinions on websites collecting and processing their information. It explored the level of trust Internet users have for relevant institutions (government bodies, banks) and their thoughts on websites' privacy policies.

- **Awareness**

  This section explored the Internet users' awareness of self-protection techniques and their perceptions of some cyber threats. These helped in making recommendations about what awareness training is necessary and helped in the design of awareness training materials.

4.3.1.2 Questionnaire Distribution

The majority of the participants were contacted through a Nigerian based research market organisation that the researcher worked with to collect the data online. A link to the questionnaire website (on qualtrics.com) was also distributed via the researcher's social network (Facebook, Twitter and Blackberry Messenger). 175 questionnaires were gathered online. A third party organisation was used mainly because of the geographical constraints. It was the most cost effective and fastest way to contact respondents based in Nigeria while the researcher was based in the United Kingdom. The use of online surveys has a number of potential advantages, for example, researchers who are using online questionnaires can get access to target participants in distant locations within a short period of time and at a low cost. This was necessary for this research because the geographical restriction.

Apart from distributing the questionnaires online, the researcher also self-administered the questionnaires. Although the self-administered method is expensive and time consuming, it enabled the researcher to explain in detail the aims and objectives of the research as well as

clarify unclear questions (Bourque, 2003). The researcher also used the opportunity to approach potential interviewees for further data collection (see 4.3.2).

The questionnaire was distributed on a university campus and in private companies in Lagos, Nigeria between February and March 2015. It was decided to conduct the study in Lagos State since Lagos is considered the commercial and industrial nerve centre of Nigeria, given its strategic location, peculiar demographics and contribution to the national GDP (Lawal, 2002). Lagos is also considered one of the most populous city in Sub-Sahara Africa (Elias and Omojola, 2015). Furthermore, Lagos is a microcosm of Nigeria because all ethnic groups are represented in the city (Oyelami, Okuboyejo and Ebiye, 2013). For these reasons, focusing on Lagos was considered appropriate for this study.

The university campus was the ideal location to get diverse group of respondents at the same place and at a faster rate. The university campus chosen was the University of Lagos (UNILAG), which is one of the major universities in Lagos. The university campus was able to provide a diverse demographic and was a location where the researcher could get access to many people at the same time, particularly young people who were of particular interest in this research (see Section 4.3.3). This approach was used to save the researcher's resources (time and money). The researcher stood in communal areas of the campus with permissions from the appropriate authority and approached groups of the respondents, describing the aim of the study and requesting their assistance in filling out the questionnaires**.**

The researcher also administered the questionnaires to private organisations that were relevant to the research, for instance, financial organisations and e-commerce companies. The main reason for this was introduce the relevant personnel to the research topic and create contacts with them for future studies. Since the researcher was based in the United Kingdom,

it was important to use the opportunity to formally introduce the research to the organisations.

The first company approached to participate in the study was a financial institution. Financial institutions are involved in providing online payment platforms for most of the e-commerce companies in Nigeria. The researcher scheduled an initial appointment with a contact in the financial institution. The contact was obtained via the researcher's former work colleagues who had previously worked for the institution. The institution is one of the major banks in Lagos and provides online payment platforms for various e-commerce companies. During the first visits, the researcher approached the contact and requested assistance in distributing the questionnaires. Ten questionnaires were distributed. However only a few were completed the same day so another day was scheduled to retrieve the rest and conduct the interviews.

The second company approached was an e-commerce company who started its business about a year before the study was conducted. As with the financial institution, the researcher was able to obtain a contact via a former work colleague. The researcher distributed five questionnaires and scheduled another visit to collect them and conduct the interview.

In some instances, the questionnaires were received immediately, however some respondants requested some time to fill them so it was necessary to come back and collect the filled questionnaires later. 45 questionnaires were filled via the paper-based method at the two companies.

4.3.2 Interviews

One of the main objectives of the research is to explore and identify Nigerian Internet users' perceptions and understanding of Internet privacy. This requires obtaining in-depth data and

information to gain insights into the issues identified in the questionnaire. This data was collected through semi-structured interviews with ten of the questionnaire participants. Section 4.3.3 provides more details of the sampling methods adopted for the interviews and questionnaire.

4.3.2.1 Semi structured Interviews

For this research, semi-structured interviews were used. Unlike a structured interview, where the interviewer is tied to a set of questions, a semi-structured interview is more flexible and aims to assist interviewers to tailor their questions to the interview context and to what the interviewee says, making it more of a conversation (Lindlof and Taylor, 2010). Hence, it offers the benefit of using a list of predetermined themes and questions as in a structured interview, while keeping enough flexibility to enable the interviewees to talk freely about any topic raised during the interview (Wahyuni, 2012). The main questions were based on the research questions and the themes discussed in the questionnaires (see Appendix A4). The interview was conducted around the same time as the questionnaires, February to March 2015.

4.3.2.2 Interview Strategy

The main strategy adopted in this research can be summarised in the following:

- Interviews were carried out at a date and time convenient for the interviewees. While distributing the questionnaires at the campuses, the researcher approached a few of the respondents and requested an interview after they had filled out the questionnaires administered. In some cases, the interview was conducted on the same day, however, in few instances, the researcher had to schedule another day to conduct the interview.

Similarly, after distributing the questionnaire at private organisations, the researcher had to schedule another meeting with the respondents that agreed to an interview.

- There are various ways of recording qualitative interviews: notes written at the time, notes written afterwards, and audiotaping (Britten, 1995).

  Rather than taping the interviews, the researcher took notes and typed them immediately after each interview..

  Although audio recording would have provided more accuracy in terms of the expressions and use of language, most of the initial participants were sceptical about being recorded and preferred note taking. The researcher decided to adopt the note-taking method for all interviewees to keep the recording of the answers consistent. The interview questions were very simple and concise, which allowed accurate notes to be taken.

  Section 4.3.3 provides more details of the sampling methods adopted for the Interviews and questionnaire.

4.3.3 Data Sampling Method

The research adopted a survey strategy using a questionnaire to investigate Nigerian Internet users' perception of Internet privacy. The sampling process involved selecting a sample of the population to investigate the study. Due to the limitations of time and resources, a sample frame was selected to represent the population. Probability and non-probability sampling are the common types of sampling (Sekaran and Bougie, 2016). A summary of methods is given in Table 4.1

Table 4.3: Data sampling methods

Probability sampling	
Simple random sampling	Each individual is chosen randomly and entirely by chance, such that each individual has the same probability of being chosen at any stage during the sampling process
Complex probability sampling	*Systematic sampling*: random selection of samples of population, every nth element. *Stratified random sampling:* population divided into groups known according to defined criteria (for example geographical areas or age groups) and then random selection of a sample from the group. *Cluster sampling*: population divided into groups based on different criteria then random selection of a sample from the group. *Area sampling*: associated with regions, random selection of samples from different regions (for example countries and villages). *Double sampling*: sub-sample chosen from first sample for further investigation and to obtain reliable results.
Non-probability sampling	
Convenience sampling	The researcher takes advantage of his/her convenience and available resources (for example contacts and position) to gather samples of participants for research.
Purposive sampling	The researcher chooses participants carefully to obtain the best sample able to provide the required information.

In this research, both probability and non-probability sampling were used as appropriate in different data collection methods. In particular, simple random sampling was used for the questionnaires. The participants were selected randomly but according to the specific criterion of Nigerian Internet users aged 18 and above. When distributing the questionnaire link, the researcher ensured that the participants' were 18 and above by including a brief message indicating the age requirement of the participants. The third party organisation that

assisted with distributing the survey was provided with the criterion before they distributed the survey online. With randomisation, a representative sample from a population provides the ability to generalise to a population, which provides minimum amount of sampling bias compared to other sampling methods (Creswell, 2013).

A convenience sampling approach was used for the interviews according to the participants' willingness to be interviewed. However, there was an element of a judgement approach, since the participants that were asked to participate were those who showed interest in the research area. This was determined when the researcher introduced the topic area and the reason for the questionnaires and judged their interest based on the rapport and the responses provided. The main reason for using this approach was to have a better understanding of the participant's responses in the questionnaire.

More focus was made on younger and educated Nigerians, as a majority of the questionnaire participants were between the ages of 20-39. This is in line with the demographic that frequently make use the Internet (Broadcasting Board of Governors, 2014). Furthermore, a study focusing on today's young Internet users provides the best chance to study the most possible widespread perceptions and behaviour in tomorrow's society regarding privacy-related issues (Miltgen and Smith, 2015). Chapter 5 provides more details about the profiles of the questionnaire and interview participants.

4.3.4 Pilot study

Before proceeding with the actual data collection, the researcher did a pilot data collection of about 70 responses. Appendix A1 shows the first version questionnaire that was used for the pilot test. A pilot study is described as a small scale replica of the main study intended to

discover possible weaknesses, inadequacies, ambiguities and problems in the research, so amendments can be made before actual data collection takes place (Sarantakos, 2005).

The pilot study participants were chosen at random but according to the specific criterion of Nigerian Internet users aged 18 and above. The researcher used social media. Links to the survey were posted on Twitter and Facebook. The pilot study data was analysed and assessed to ensure the main outcomes of the analysis served the main goals of the research and that it worked as intended. Hence, after reviewing and analysing the questionnaires from the pilot study, certain questions were refined and some of the questions were shortened to prevent ambiguity and misunderstanding.

4.3.5 Content Analysis

Content analysis is the systematisation of text analysis. Underlying meanings and ideas are discovered through examining patterns in elements of the text, such as words or phrases (Holsti, 1969). Content analysis can contain aspects of either qualitative or quantitative methodology. It can be focused on word counts, which gives it quantitative features. It can also be focused on word meanings, such as metaphors, to provide the cultural context in which texts are produced and this gives it qualitative features (Berelson, 1952; Holsti, 1969).

Hsieh and Shannon (2005) described three approaches to content analyses. The first is conventional content analysis and is generally used with a study plan to describe a phenomenon. This type of plan is usually appropriate when existing theory or research literature on a phenomenon is limited. The second is a directed approach, which is used when a prior theory or research exists about a phenomenon that would benefit from further description. The third is a summative approach, which is used to identify and quantify certain words or content in a text with the purpose of understanding the contextual use of the

words or content. This approach is used for data collection in this research. Content analysis was used to analyse websites' privacy policies and data collection practices; the results were analysed qualitatively. It was also used to analyse different data protection approaches to determine their applicability in Nigeria (see Chapter 5 and 6).

4.4 Data Analysis

The collected data are in two forms, quantitative and qualitative. In the quantitative data, statistical analysis was used to analyse relationships between the variables.

Using the analysis feature of Qualtrics©, the demographics of the participants and the frequency of their responses were tabulated. The Qualtrics© software provided the statistical results based on the software's criteria for completed surveys. Qualtrics© is a software package with strong statistical functions available. The package also provides data in numerical tables and graphs.

Qualitative data are usually in the form of statements and comments, it needs to be analysed with a different approach. A common approach to the interpretation of meanings from textual data is using thematic analysis. Thematic analysis involves searching across a data set (for example a number of interviews or focus groups, or a range of texts) to find repeated patterns of meaning (Braun and Clarke, 2006). A theme is a pattern found in the information that, at a minimum, describes and organises the possible observations and at a maximum interprets aspects of the phenomenon (Boyatzis, 1998). A theme captures something important about the data in relation to the research question and represents some level of patterned response or meaning within the data set (Braun and Clarke, 2006). Through the first step, researchers read and re-read the data, transcribing if necessary, to become familiar with the depth and breadth of their data (Braun and Clarke, 2006). The second step is to code all the basic units

of the text that seem important such as words, phrases, sentences, paragraphs, sections, chapters, and books and place them into initial code categories. Coding is determined from the aims of researchers and the topic they want to investigate. Coding can be done manually or through software. This study used manual coding.

Software such as NVivo helps researchers manage, store and analyse large quantities of data (Basit, 2003) as it is a useful tool to link the data to emerging concepts and themes. However, it does not replace the researcher's role in analysing and interpreting the data (Morse *et al.,* 2002). The manual approach employed in this research project encouraged a close relationship between the researcher and the data. Furthermore, it was considered manageable to code manually since not many interviews were conducted.

4.5 Conclusion

This chapter describes the research methodology applied in this research, starting from the adoption of the appropriate philosophy and research approach. For this research a mixed methods approach was used with elements of both positivism and interpretivism. The chapter also discusses the choice of sampling methods for each data collection method applied in this research, using both probability and non-probability approaches.

Subsequently, a detailed description of the chosen data collection methods is presented. Using a quantitative approach, questionnaire data were analysed using the Qualtrics software while a qualitative approach with data from semi-structured interviews was analysed manually. The research also used content analysis as a data collection method, which was then investigated with a thematic analysis.

Chapter 5 discusses the study conducted to find out which websites have good privacy and data protection practices by analysing their policy content.

Chapter 5: Nigerians' Perceptions of Personal Data Protection and Privacy

The chapter analyses the public understanding and knowledge of data protection and Internet privacy in Nigeria via surveys and interviews. First, it considers the understanding of the implication of disclosing personal information. Perceptions of privacy and data protection are then considered in light of what information is considered personal and generally causes concern when asked to provide it. The general perception of purchasing online is investigated and how concerned Nigerians are about providing personal details when purchasing online. This is followed by the public's perception of current data protection practices in Nigeria. The level of privacy concern about organisations' use of personal information, policies on sharing information with third party organisations, and the level of trust in government and private companies are considered. Finally, the public's level of awareness of the repercussion of bad privacy, data protection practices and individual self-protection methods are considered.

5.1 The Conceptual Framework and Hypotheses

The influx of e-commerce in Nigeria has resulted in individuals shopping online and sharing personal information about themselves and their family, friends and colleagues. A survey and interviews were conducted in this research to gain an initial understanding of attitudes about privacy among Nigerians and their understanding of e-commerce data protection and privacy. This section describes the conceptual framework and the hypotheses used to carry out the study.

Cultural values and privacy perceptions differ from country to country. These varying values exert a significant influence over how privacy is respected and treated in a given country. This, in turn, determines what data protection approaches a country adopts or if a country has effective data protection (Rudraswamy and Vance, 2001; Wolf Park and Digital Jewels, 2014). Factors, such as the political changes in a country, economic priorities and the public's perception of personal information and its protection, can affect how privacy is viewed which then influences the adopted privacy policy.

Hypothesis one: The current views of privacy are focussed mainly on financial aspects and knowledge of other aspects of privacy protection is insufficient.

Some nations may or may not be overly concerned about the need for data protection to protect their citizens or corporations. This is notable in the case of developing African nations, such as Nigeria, that lack privacy protection legislation. Studies have shown that regulatory responses usually occur in reaction to a growing level of information security concern within the masses (Rudraswamy and Vance, 2001; Chiejina and Olamide, 2014). Nigeria is known for its high level of cybercrime, so many Nigerians are becoming aware of the dangers of putting credit/debit card details on just any website (Akinsuyi, 2010), this has prompted many e-commerce websites to adopt the pay on delivery method (Chiejina and Olamide, 2014). This method provides peace of mind as no bank or card details are compromised. However, is there still the danger of personal identifiable information misuse? This study supports the suggestion that the current views of privacy are focussed mainly on financial aspects, and knowledge of other aspects of privacy protection is insufficient.

Hypothesis two: The public generally shows higher levels of trust in private bodies rather than in the government to protect their privacy interest.

The government has endorsed draft guidelines on data protection and cyber-security in the past, but there is yet to be any legislation and there is no immediate prospect on anything being passed as a law (Akinsuyi, 2010). According to a survey by Transparency International (Transparency International, 2015). 73% of the Nigerian population believes that the Nigeria legislative and parliamentary body is opaque and corrupt. Nigeria, being a developing economy, is striving to provide the basic infrastructure of a steady supply of electricity, good roads and transportation, health, education services and postal and telecommunication networks (Uma and Eboh, 2013). Considering this, it is safe to say that the enactment of a working data protection policy would not be the government's priority.

Hypothesis three: Many people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it

One of the repercussions of bad data protection and privacy practices is identity theft. Apart from companies or government protecting the privacy interest, there should be awareness of self-protection methods. The lack of user awareness of these methods could lead to identity theft.

5.2 Research Methods

The study included a questionnaire and semi-structured interviews. The methodology used for the study is explained in Section 5.2.1

5.2.1 Questionnaire

A questionnaire was developed with the goal of collecting opinion-based information from individuals who reside in Nigeria. Web and paper-based collection channels were used to make completion of the questionnaire as convenient as possible (see appendix A2 for

questions). Section 4.3.1 provides more details on how the questions were developed. A link to the questionnaire website (on qualtrics.com) was distributed via a private survey company and the researcher's social network (Facebook, Twitter and Blackberry Messenger). 175 questionnaires were gathered.

The paper-based questionnaires were distributed on a university campus and in private companies. A total of 45 paper questionnaires were collected. The private companies interviewed were a bank well known for providing payment services for e-commerce websites and an e-commerce company. The researcher used this opportunity to introduce the research to them and create contacts with them for future studies. The researcher chose the university campus because it was one of the few places to get good number of people at the same time. A grand total of 220 questionnaires were used for the study. Section 4.3.3 provides more details about the sampling and approach used

Table 5.1: Description of respondents' characteristics

Characteristics	**Value as a percentage of N=220**
	Percentage
Gender	
Male	53%
Female	47%
Age	
<20	11%
20-29	58%
30-39	21%
40-49	7%
>50	3%
Education Qualifications	
PhD	3%
Masters	20%
Bachelors	42%
Undergraduate	34%
School Certification	1%

To keep the questionnaire form short, only those items crucial to the research objectives were included. Hence, key items focused on individual perceptions about institutions that collect and use personal information and general perceptions of personal information. More focus was made on younger and educated Nigerians. The main reason for this is that the majority of those who regularly use the Internet are within the age range of 15-24 and have post-secondary education (Broadcasting Board of Governors, 2014) and may well have different views on and approaches to the disclosure of personal information to those who rarely use the Internet. Table 5.1 summarises the demography of the sample. The Qualtrics survey tool was used to analyse the results.

5.2.2 Interviews

Brief one-on-one semi-structured interviews were conducted to get an in-depth and personal view of the individual. 10 of the questionnaire respondents were chosen based on their interest in the research and their willingness to participate in the study**.** Section 4.3.3 provides more details of the sampling process used to choose the interview participants. No personal information such as names or email addresses that would identify any individual was collected. The interviews contained questions that provided more detailed information about views on providing personal information while performing online transactions, on government's involvement in data protection and on website policy documents. The interviews took place after respondents finished answering the questionnaire questions and were conducted in Lagos. All interviewees were between the ages of 18 and 39 (5 were in their thirties, 4 were in their twenties and 1 was below the age of 20). An opportunistic approach was used to determine which of the participants were chosen for the interview based on the availability of the participants and their interest in the research topic.

5.3 Questionnaire Analysis

This section presents the analysis of general perceptions of purchasing online, comfort levels for sharing different types of data online, trust in businesses and government, and third party information sharing. The chi-squared test was applied to show the relationships between the responses gathered (see Appendix A for the full results).

5.3.1 Importance of Personal Information

The disclosure of personal information seems to have become an increasingly common part of everyday life. It can be open and deliberate in some cases, in exchange for services, or unintentional and hidden, for example when behaviour is being tracked through websites, mobile phones or credit cards (Sarathy and Robertson, 2003b). One of the aims of the questionnaire and interviews was to determine what people consider personal information that they would not easily disclose. This section (5.3.1) examines Nigerians' disclosure of personal information, what they consider to be personal information, and how they feel about disclosing their personal information online.

5.3.1.1 Information Considered as Personal

Respondents were asked how comfortable they were providing specific information to web sites. There are significant differences in the comfort levels for different types of information. Respondents were most comfortable sharing their gender, email address, religion, Facebook address and occupation with web sites. They were least comfortable sharing financial information (bank account details, debit/credit card number, annual income), home address number, health and medical history. See table 5.2 for results summary.

Table 5.2: Which of the following Information is personal and you feel uncomfortable sharing?

	%
Financial Information (bank account details, credit/debit card details,	92.54%
Health/Medical Information	41.79%
Passport Number	34.83%
Home address	59.20%
Mobile/landline number	42.29%
Photograph	15.42%
Full name	14.43%
Email address	6.47%
Facebook address	7.96%
Age	62.19%
Marital status	16.92%
Religion	8.46%
Gender	4.98%
Occupation	2.99%

5.3.1.2 Disclosing Personal Information during Online Transactions

All respondents were asked if they performed transactions online. The general finding is that some of the participants are sceptical about performing transaction online with nearly half the respondents only occasionally or never doing so.

Table 5.3: Do you perform transactions online?

Answer	%
Always	18.81%
Most of the Time	16.83%
Sometimes	30.69%
Rarely	21.29%
Never	12.38%

Interestingly, 82% of the respondents agree that disclosing personal information is necessary and increasingly part of modern life.

The chi-squared test shows also a clear relationship between the respondents wanting to purchase online and disclosing personal information, (The p-value is .00007. The result is significant at $p < .05$).

5.3.2 Protection of Personal Information

Companies holding personal information may sometimes use it for a purpose other than that for which it was collected. Surprisingly a larger percentage of respondents were not concerned about this. The survey asked questions to determine their opinions on e-commerce websites collecting and processing their information.

5.3.2.1 Trust in Institutions

To understand the level of trust Nigerians have in institutions involved in e-commerce, they were asked to what extent they trusted them to protect their personal information. Table 5.4 shows that the majority of respondents (71%) trust private institutions and a general lack of trust is shown towards government institutions and e-commerce websites.

Table 5.4: To what extent do you trust the following institutions to protect your personal information?

Question	Total trust	Somewhat trust	Do not trust
E-commerce websites	16.85%	56.74%	26.40%
Banking and financial institution	70.74%	28.19%	1.06%
Government or public institution	14.00%	26.67%	59.33%

The chi-squared test shows a relationship between respondents who trust e-commerce websites and those who are comfortable performing online transactions. (The p-value is .000015. The result is significant at $p < .05$).

5.3.3 Awareness

Everywhere Internet users make use of information services, they leave traces making it possible for anybody who is interested to collect and analyse our personal data. Hacking with the purpose of stealing confidential data is a very common cyber-attack known today. Once a user's account is compromised, there could be ramifications such as identity theft. A hacker can gain access to very confidential information such as bank account and credit/debit card details, home addresses and so on.

5.3.3.1 Identity Theft Awareness

The respondents were asked if they considered identity theft a threat when online. The majority of the respondents (72%) were aware of identity theft and the threat it poses. This is depicted in Table 5.5

Table 5.5: Are you aware of Identity theft and its repercussions?

Answer	**%**
Yes	72.36%
Not sure	26.63%
No	1.01%

5.3.3.2 Self-Protection Techniques

Respondents were asked about awareness of some common privacy enhancing techniques. Table 5.6 shows that the most common awareness was about antivirus software and deleting cookies, but the majority were not aware of any techniques at all.

Table 5.6: Which of the following privacy-enhancing techniques are you aware of?

Answer	%
Deleting cookies	16.16%
Altering browser settings	11.11%
Providing false information on websites	11.62%
Antivirus software	17.68%
Check for https on the website	8.59%
Check for security logo or web seals	16.16%
None	64.65%

The chi-squared test shows clearly a relation between levels of awareness with age (The p-value is .00007. The result is significant at $p < .05$). Responses show that the majority of those who did not know about privacy enhancing techniques were aged 30 and above.

5.4 Interview Analysis

Semi-structured interviews were used in conjunction with the questionnaire to aid better interpretation of results (see Section 5.2.2). The interviews created an avenue to ask for further clarification of certain issues and assisted in gathering additional information that were not captured by the survey.

Table 5.7: Profile of Interviewees

Characteristics	Value as a percentage of N=10
Gender	
Male	60%
Female	40%
Age	
<20	10%
20-29	40%
30-39	50%

5.4.1 Disclosing Personal Information Online

The 10 interviewees were asked if they felt comfortable providing their information when performing transactions.

All of the interviewees regularly use the Internet and perform online transactions. Six out of ten interviewees had no problems providing their personal information when performing transactions. Four indicated they had no issues disclosing their information if they are familiar with and trust the website. All the interviewees stated that debit/credit card details are the information they feel least comfortable providing when purchasing goods and services online.

5.4.2 Reading Website Policies

Eight of the interviewees indicated that they never bother to read website policies and two said they read them on occasion. The most prevalent reasons for not reading them are that they are lengthy and difficult to understand. Only one of the interviewees said they read a website's return policy and reviews on the website to verify the authenticity.

5.4.3 Trust in Government

The interviewees were asked if the Nigerian government could be trusted to handle privacy and data protection affairs. A brief explanation about the current data protection approach in the United Kingdom was given for more understanding. Six of the interviewee stated that the government could not be fully trusted to handle the nation's privacy and data protection needs. Three indicated that they can be trusted and one was not sure. One of the interviewees added that they are sure that the government has or is planning to have a data protection system but they are also sure that it will not be in any way effective or reliable. Another of the interviewees stated that the government simply is not ready to fully handle privacy issues

but probably would be some time in the future. All of the interviewees agreed that the website owners and the bank should be responsible for protecting customer's information.

5.5 Conclusion

This study was undertaken to understand the attitudes of Nigerians about privacy through a written survey and interviews.

Most of the survey respondents felt their financial information (bank account details) was the most important personal information. It was found that most of the interviewees felt least comfortable providing their credit/debit card details when performing transactions online. This could be the reason why the pay-on-delivery payment option is becoming the most popular payment option among the respondents (55%) and Nigeria (Chiejina and Olamide, 2014). However, it is important to note that many of the respondents were still comfortable with the credit/debit card payment method. This could be because the banks solely manage the online payments of e-commerce websites in Nigeria with these websites linking to the bank's website to handle the payment rather than handling the transaction themselves. The banks in Nigeria are a relatively effective institution and seem to command the trust of the population. This supports the first hypothesis that state that the current views of Personal Identifiable Information privacy are focussed mainly on financial aspects and knowledge of other aspects of privacy protection is insufficient. It is apparent that the public places value on the idea of privacy and data protection, but the only real concern is for financial information.

Most of the respondents disagreed that the government can be trusted to look after the citizens' privacy interests. This distrust may have originated from the government's inability to enact any legislation. Generally, private institutions such as banks and to a certain extent,

the e-commerce website, are perceived as being the major regulatory body in terms of Nigerian e-commerce. This fully supports the second hypothesis that states that the public generally show higher levels of trust in private bodies rather than in the government to protect their privacy interest.

There is a good awareness of identity theft amongst respondents. Most of those that were aware of self-protection techniques were aware that they could delete cookies, and install antivirus software but many were not aware of any preventive techniques. The awareness of identity theft exists, but there seems to be a lack of appreciation of the dangers of this type of theft and that leaves the population very vulnerable. This supports the third hypothesis that states that many people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it.

In general, a majority have accepted the disclosure of personal information is necessary for e-commerce but appear to be minimally concerned about providing information unless financial information is concerned. The advantage of there being little concern about companies misusing their personal information is that this could lead to a rapid growth of e-commerce. However, the downside is that their lack of concern could mean that the Nigerians are vulnerable to their information being misused.

Steps should be taken to make the Nigerian people more aware of their vulnerability to theft of their personal and private information. Clearly, the government of Nigeria do not have the time and resource to put in place effective legislation to protect the citizens against identity theft, but in any case, even if they did so, the population would not trust them to sufficiently enforce this legislation (see Chapter 7). Nigerians need to realise that identity theft could be a serious danger and they need to be shown how to protect themselves. This would then help

protect the population until effective laws and enforcement is possible. This recommendation will be discussed in more detail in Chapters 9 and 10.

Chapter 6: Analysis of Data Protection and Privacy Practices in Nigeria

Chapter 5 discussed Nigerians' perception of personal data protection and privacy and how there is a general lack of awareness and concern for privacy issues. This chapter analyses the privacy practices of Nigerian websites.

Internet users rely more and more on the convenience and flexibility of the Internet to shop, communicate and in general perform tasks that would otherwise require a physical presence (Provos *et al.,* 2007). The Internet, which ordinarily is supposed to be advantageous particularly to a developing nation's economy, could become a source of uneasiness due to the high level of cybercrime and lack of initiatives to combat this issue (Ehimen and Bola, 2010). It is, therefore, the responsibility of the websites to practice good privacy practices in order to ensure customers' information is safe and improve e-commerce trust. Studies have shown that trust of online businesses can be enhanced through privacy policies, and by paying attention to the security of private information that is collected (Earp and Baumer, 2003; Jakovljević, 2011). A privacy policy is a comprehensive description of a websites' information and privacy practices, usually located in an easily accessible place on the site. These policies are typically the only information source available to consumers who are deciding whether or not to communicate with the website (Federal Trade Commission, 2000).

This chapter discusses the study conducted to find out which websites have good privacy and data protection practices by analysing their policy content. In addition, a web crawler, a tool designed to record and analyse online data practices, was used to gather data from these websites. Compliance of the website can be verified by examination of the website's privacy policy and their actual practices.

Several aspects of privacy policies in Nigerian e-commerce websites were examined in order to understand the general privacy practices in Nigeria. The results from this study can help determine general privacy practices of Nigerian websites and also help develop recommendations for practices to improve e-commerce and online trust in Nigeria. This chapter is organised as follows: First, it covers the description of Fair Information Practices and its applicability to privacy policies. Second, a study is made of Nigerian Internet web sites and the benefits of privacy policies in building trust in e-commerce. Finally, it discusses the results of the study, highlights the implications for Nigerian E-commerce and makes recommendations for improving the sites.

6.1 Privacy Policies and Trust in E-commerce

A lot of research has shown the importance of trust in an online context. In e-commerce, trust has been shown to have an important positive influence on its growth (Bart *et al.,* 2005; Cyr, 2014; Seckler *et al.,* 2015). Most online businesses make use of customers' data to track customers' behaviour. When the customer makes a transaction, then the organisation might store the user's name, address, phone number, e-mail or credit card information. The organisation can then use these data to provide customised advertising and personalised services, building strategic relationships with customers (Sarathy and Robertson, 2003b). Nonetheless, customers are concerned about their personal information being misused, for instance being given to third party organisations. Internet users will look for indications that a website is trustworthy before engaging in e-commerce (Earp and Baumer, 2003). These include posted statements or privacy policies that provide information about what the organisation will do with their personal information. A website adopting fair procedures to protect customers' privacy develops business-customer trust, so customers are likely to be

more willing to disclose personal information. If all websites adopt fair procedures, the outcome is a rapid development of e-commerce and Internet adoption.

6.1.1 Privacy Protection Goal Taxonomy Classifications

Anton and Earp (2004) conducted a study by introducing taxonomy of privacy protection goals making use of goal-driven requirements engineering that provides an effective mechanism for analysing and comparing privacy policies. They employed a content analysis technique and goal mining to derive the privacy-related goals of various care web sites.

The goals were obtained from Internet e-commerce privacy policies and were categorised according to common characteristics that emerged and were coded into the Fair Information Practices. This is described in table 6.1.

Table 6.1: Privacy protection goal taxonomy

Privacy Protection Goal Taxonomy	**Goal Sub-Classifications**
Notice/Awareness Goals asserting that consumers should be notified and/or made aware of an organisations information practices before any information is actually collected from them (for example an organisations privacy policy).	Identification of the uses to which the data will be put Identification of any potential recipients of the data 3rd party limitations Nature of the data collected Steps taken by the data collector to ensure the confidentiality, integrity, & quality of the data
Choice/Consent Goals ensuring that consumers are given the option to decide what personal information collected about them is to be used for and whether it may be used for secondary purposes.	Choice of how data is used Choice of sharing data Choice of what data is taken/stored

Access/Participation Goals allowing or restricting access to a particular site or functionality based on whether or not the consumer provides their PII. Goals in this category address also the ability for consumers to access or correct any personally identifiable information about themselves.	PII provision required PII provision optional Providing consumer access to data
Integrity/Security Goals ensuring that data are both accurate and secure. Security and accuracy comes from both the consumer and the organisation collecting the PII. Goals in this category range from vague statements stating only that PII is kept securely to specific technical goals of what security protocols will be used to transfer PII over the Internet.	Mission statement User-supplied integrity goals Using anonymous PII Destroying untimely or sensitive data Managerial measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data Technical measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data
Enforcement/Redress Goals addressing the mechanisms that are in place to enforce privacy, otherwise a policy is merely suggestive, rather than prescriptive. Prescribe a way of working and general guidelines companies should follow. These include both self-imposed and government imposed work restrictions.	Operational prevention assurance 3rd party prevention assurance Failure of assurance

6.1.2 Vulnerabilities of Websites in Nigeria

The introduction of Internet, although having a lot of advantages, also introduced an exceptional outbreak of cybercrime in Nigeria and the impact on the socio economy of the country is highly alarming (Ibikunle and Eweniyi, 2013). It also doesn't help that Nigeria is operating on a weakened technology platform and digitally illiterate environment and is in

urgent need of expert and effective cyber-security policies (Adewole, Olayemi and Isiaka, 2011).

A study by (Suleiman *et al.,* 2015) examined the vulnerabilities of 25 websites owned by various organisations in Nigeria from across different sectors that handle sensitive data, which led to them suggesting techniques for software developers to prevent such risks. They conducted a risk analysis by using OWASP ZAP (open-source web application security scanner Zed Attack Proxy) to test for risk of penetration and categorised the risk into three levels that will identify weaknesses in website coding. It was revealed that although the high-risk sites were very few, there were still significant numbers of medium and low risks alerts. Suleiman et al. suggested that developers in Nigeria still have room for improvement in security when it comes to design and development of such applications. They also provided recommendations to address security challenges to match the website security of other developed nations.

The study conducted by Suleiman et al. (2015) explores the technical deficiencies of Nigerian websites. The study used in the research described in this thesis uses content analysis methods to analyse the privacy practices and data collection practices. Section 6.2 describes the website analysis carried out, the results and the implications

6.2 Analysis of Nigerian Websites

A study was carried out on 65 Nigerian websites by analysing their content and data collection practices. The websites were chosen from Vconnect (Vconnect, 2017), a local search engine and an information service provider company, similar to Yell. The websites used for this study are considered the most active and popular website according to Vconnect (2017). This was chosen because the researcher reasoned that, given their popularity, those

websites would have comprehensive privacy policies. The list of the websites used for this research is in Appendix D.

6.2.1 Content Analysis

Data was collected from 65 Nigeria e-commerce websites by manual review of the website policies and cookie checkers. For each privacy policy, practices based on the Fair Information Practices were investigated. The study does not focus on readability of policies, but their actual content. The researcher read through the text and manually identified practices by focusing on key words related to privacy practices as described in Table 6.1. This is further described in sub-sections 6.2.1.1 to 6.2.1.4:

6.2.1.1 Notice and Awareness

The notice and awareness principle states that consumers should be notified and/or made aware of an organization's information practices before any information is actually collected from them. Website's visitors are usually made aware of such practices in a site's privacy policy. The following statements about notice and awareness were looked for in the privacy policies:

- Identification of the organisation collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- Nature of the data collected;
- Means by which data are collected (if not obvious);
- Whether the provision of the requested data is voluntary; and

- Steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

6.2.1.2 Choice and Consent

The choice and consent principle ensures that consumers are given the option to decide what personal information collected about them is used and whether it may be used for secondary purposes. The following statements about choice and consent were looked for in the privacy policies:

- Opt in
- Opt out

6.2.1.3 Access/Participation

The principle of access and participation asserts that consumers are able to access, correct and challenge any data about themselves. The study will look for information that the website

- Allows customers to modify/remove their PII

6.2.1.4 Integrity/Security

Integrity and security goals reflect the ways in which a Web site ensures that data is both accurate and secure. This focuses on protecting sensitive data via managerial or technical measures. Statements containing the following information were looked for in the policies:

- Managerial measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data
- The destroying of untimely or sensitive data

- Technical measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data
- The provision of customer access to data.

6.2.2 Data Collection Practices

The study also investigated the data collection practices of the website. Cookie checkers were used to record the use of the website's own cookie, as well as any third-party, cookies. The privacy policies of these Web sites were reviewed to look for information about cookie usage and the use of third-party cookies. Attempting to register or initiate a transaction on the websites also identified the use of cookies. The cookies revealed by the cookie checkers were manually inspected and tabulated. Figure 6.1 shows the cookie summary result for jumia.com.ng, a popular Nigerian website.

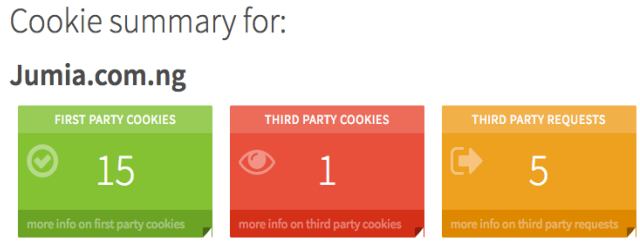

Figure 6.1: Cookie summary for a Nigerian website

The policies were also checked to see if they disclose the presence of cookies and third party cookies. Table 6.2 shows the data collection practices that were inspected.

Table 6.2: Data collection practices

Data Collection	Use cookies to track user behaviour Disclose that the Web site is using cookies Explain what cookies are Explain how to turn off/decline cookies
Third-Party Data Collection	Allow third parties to use cookies on the Web site Disclose the presence of third party cookies on the Web site Provide a link to the privacy policy of the third party

6.3 Results

This section describes the results from the study conducted in Section 6.2

6.3.1 Policy Content Analysis

The results will be grouped into four categories based on the practices defined in the taxonomy in table 6.1. The results are summarised in Table 6.3.

Table 6.3: Content analysis results of Nigerian website

Privacy Practices	**N=65**
Notice and Awareness	
Identification of the entity collecting the data	97%
Identification of any potential recipients of the data	76%
Nature of the data collected	89%
Means by which data is collected	68%
Whether the provision of the requested data is voluntary	59%
Disclose how data are used for internal transaction processing	47%
Disclose how data are used for internal marketing purposes	58%
Disclose how data are used for outsourced transaction processing by a third party	25%
Disclose how data are used for marketing purposes by third parties	34%
Choice and Consent	
Provides opt in options	45%
Provides opt out options	68%
Access and Participation	
Allow customer to modify/remove their PII	43%
Provide customer access to data	43%
Integrity/Security	
Managerial measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data	37%
Technical measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data	66%
Destroying untimely or sensitive data	9%

Since a privacy policy acts as a signal to the user, it should relay information that is of importance to users. According to the results, generally, most websites place more importance on notice and awareness. This is a very important privacy practice because it suggests consumers should be notified and/or made aware of an organisation's information practices before any information is actually collected from them. Even though importance is placed on disclosing who is collecting the data and what the nature of the data collected, little importance is placed on disclosing how data is being used internally for transactions and marketing purposes with just 47% and 58% disclosing this, respectively. This is much lower for disclosing how data is being used by third parties for transaction and marketing purposes with just 25% and 34% disclosing this, respectively.

The practice given second highest importance is the category of Choice/Consent, for statements about the user being able to decide what information about them can be used. These are usually in the form of providing information with opt-in and opt-out options. However, the percentage of websites which disclose information about this practice is low with just 45% disclosing information about opt-in procedures and 68% disclosing information about opt-out procedures.

The practice of access and participation that states consumers should be able to access, correct and challenge any data about them was not given much importance by the e-commerce websites as 43% of the websites indicated that they would allow and provide information on how customers could gain access to their data.

The category given the least importance was Integrity/Security, or statements assuring security for data collection and transfer. Although a significant 66% of sites provided information about their technical measures, just 37% provided information about their

managerial measures.

Section 6.4 discusses the results of the study in more detail.

6.3.2 Data Collection Practices

The study also investigated the data collection practices of the website by investigating their cookie usage and the use of third-party cookies. Although there are other ways a website could collect data, such as pop-ups, web bugs, and so on, the study focused on cookies because of their common use. The results are summarised in Table 6.4.

Table 6.4: Data collection practices

Data Collection Practices	**N=65**
Use cookies to track user behavior	97%
Disclose that Web site is using cookies	52%
Explain what cookies are	38%
Explain how to turn off/decline cookies	17%
Disclose the presence of third-party cookies on the Web site	16%

The cookies recorded for the various website were inspected to see whether they were placed by the visited website or by a third party operating from that website. Most of the websites (97%) used cookies on their websites but just 52% disclosed their cookie usage. Third parties placed cookies on 78% of the websites. Of these websites, 16% disclosed the presence of these third party cookies on their website. Few websites explained what cookies are and how to decline them (38% and 17%, respectively). Section 6.4 discusses the results in detail.

6.4 Discussions and Conclusions

It is important for customers to understand the risks of providing their information online including the prevalence of undesirable or dubious security and privacy practices in order to make better decisions about whom to trust. Although this is an important concept, the majority of personal data collected by websites is done through direct means of user entry, so users may already be aware of much of the information that is being collected. Nevertheless, the content analysis has revealed that these websites' policies fail to provide information about important areas of privacy. It was discovered that most of these websites are silent with regard to important consumer-relevant practices, including how the data being collected are used internally and by third parties. Many of policies also did not provide information about opt-in and opt out procedures, which give customers control of what data they would provide. It is possible that these websites might have opt-in and opt-out procedures but it would be good practice to include details about this in their policy documents.

Surprisingly, few websites provided information about their technological and managerial measures to protect customers' data. Sensitive information such as financial information is a major concern for Nigerian Internet users Although, it is typical for websites to employ some security measures to protect their data, it is also important to provide information about this practice to put customers' minds at ease. Such knowledge can help them adopt effective and necessary safeguard mechanisms.

The data collection practices of the websites were also evaluated. It was discovered that although the majority of the websites make use of cookies and third party cookies, many fail to disclose information about this practice. Overall most of the websites fail to adequately fulfill the general guidelines for good privacy practices and significant improvements are needed in this regard.

This limitation could be because of the current lack of efficient enforcement and monitoring of good practice. It can be suggested that standards and principles tailored to the current e-commerce industry in Nigeria are needed. The standards should include compliance monitoring and enforcement for e-commerce websites to encourage good privacy and disclosure practices. The next chapter (Chapter 7) conducts a study to determine if a regulatory approach would be applicable in Nigeria. The chapter compares both self and government regulatory approaches.

Chapter 7: Interpretation of Government and Self-Regulation Data Protection Approaches in Nigeria

Many online businesses make use of customers' personal data to provide customised advertising, personalised services and strategic relationships with customers. According to the UK Data Protection Act (Legislation, 2016), "Personal Data" is defined as "Data that relates to a living individual who can be identified from such data, or /and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

Some customers are concerned about their personal data being used inappropriately, and this could reduce customers' trust in the website's services (Sarathy and Robertson, 2003b). Fear about privacy and the lack of trust continue to be the biggest obstacles to the growth of e-commerce. These developments have forced several nations of the world to enact legislation and procedures to protect the information privacy of their citizens and corporations.

The European Union in 1995 decided to adopt formal enforcement in the form of the Data Protection Act (Legislation, 2016) incorporating the eight OECD principles (see Chapter 2, Section 2.2), while the United States, although endorsing the principles, adopted the self-regulation approach rather than governmental regulation (Cate and Mayer-Schönberger, 2013). In Nigeria's case there is yet to be any fully functioning government enforcement and self-regulatory system. There have been a number of drafted bills for e-commerce personal data protection, but they are yet to be effective (Akomolede, 2008).

The government and self-regulation approaches are evaluated in detail in this chapter to determine whether they may be effective or not in developing nations. This chapter investigates the reasons why developed countries adopt any particular system for data protection. It also evaluates these data protection approaches to determine its applicability in developing nations, using Nigeria as a case study. This is achieved by identifying the issues affecting data protection in the developing country and then evaluating the approaches' dispute resolution, enforcement and compliance monitoring processes for their applicability in the case of Nigeria. Benchmarks developed by the Australian government for Industry-Based Customer Dispute Resolution Schemes provide a suitable mechanism for evaluation and these also cover the common content of international dispute resolution standards (Cavoukian and Crompton, 2000). They provide good practice guidelines for organisations, with dispute resolution procedures and serve as a guide for customers in giving them some idea of what they should expect from the organisation. Therefore, the guidelines are suitable for determining the effectiveness of the processes that any data protection approach should perform: consumer dispute resolution, compliance monitoring and enforcement.

7.1 Factors affecting a nation's data protection approach

Cultural values and privacy perceptions differ from country to country (Sarathy and Robertson, 2003a; Milberg *et al.,* 1995). These varying values exert a significant influence over how privacy is respected and treated in a given country. This, in turn, determines which data protection approaches a country adopts or if a country has effective data protection (see Chapter 2 for definitions of different data protection approaches). For example, the European Union's adoption of Europe-wide governmental regulation for protecting consumer data privacy may be interpreted as a reaction to the excesses of various oppressive regimes in the earlier part of the twentieth century, especially during World War Two, and the continuing

fear of the misuse of personal data by corporate and government entities (Sarathy and Robertson, 2003b). The United States has leaned towards industry self-regulation, which could be rooted in the country's history of entrepreneurial behaviour and laissez-faire capitalism (Sarathy and Robertson, 2003a).

Factors, such as the political changes in a country, can affect how privacy is viewed which influences the adopted privacy policy. Not all countries subscribe to the notion of privacy as a fundamental human right, which impacts the way a nation accepts the need to protect individual privacy rights. A nation's unique situation and issues of government, culture and even history should be considered for the implementation of a working data protection approach.

7.1.1 Issues Affecting Data Protection in Nigeria

Nigeria has not yet enacted any specific data protection law. Some other African countries, such as Ghana, South Africa and Egypt, are ahead of Nigeria in implementing data protection policies (National Information Technology Development Agency, 2013). A draft guideline on a data protection bill was published by Nigeria's National Information Technology Development Agency (NITDA) in 2013 but it has not been passed into law and there is no establishment of an institutional framework (Transparency International, 2015).

A new cybercrime bill was introduced in 2013 with an update of provisions to the previous Computer Security and Critical Information Infrastructure Protection Bill of 2005 (ngCert, 2014). The draft legislation imposes certain security obligations on organisations operating computer systems and networks, but does not sufficiently address data protection (Transparency International, 2015).

As initially mentioned, a nation's socio-cultural and economic factors can determine a

nation's regulatory approach. There are also reasons why a country may not view e-commerce data protection as a priority. Six suggested Nigerian factors that influence the inadequate data protection are discussed in this section. These affect many, if not most, developing countries; the last is more particular to Nigeria.

7.1.1.1 Government Enforcement

Nigeria does not have a specific data protection law and there is not any functional self-regulatory system (Akomolede, 2008). Although a new cybercrime bill was introduced in 2013, it does not sufficiently address data protection (Chiejina and Olamide, 2014).

According to a survey carried out by Transparency International (Transparency International, 2015), 73% of the Nigerian population believes that the Nigeria legislative and parliamentary body is opaque and corrupt. This implies that even if legislation were enforced the population would not have confidence that it would be enforced effectively.

7.1.1.2 Political History

The political views of a country can affect its view on data protection (Steinke, 2002). Nigeria's military regime has played a major role in the country's history, often seizing control of the country and ruling it for long periods of time. Data protection and Fair Information Practice may not be widely accepted by totalitarian regimes. Although there was a political regime change in 1999 to democracy, the long-term totalitarian regime and the resulting ingrained attitudes could be a factor influencing the nation's slow adoption of a data protection policy.

7.1.1.3 Economic priorities

Nigeria, being a developing economy, is striving to provide the basic infrastructure of a steady supply of electricity, good roads and transportation, health, education services and

postal and telecommunication networks and so on (Uma and Eboh, 2013). The enactment of a data protection policy would not be the government's highest priority.

7.1.1.4 Importance of personal Information and Information security

Some nations may or may not be overly concerned about the need for data protection to protect their citizens or corporations (Rudraswamy and Vance, 2001). This is notable in the case of developing African nations, such as Nigeria, which lack privacy protection legislation. Studies have shown that regulatory responses usually occur in reaction to a growing level of information security concern within the masses (Rudraswamy and Vance, 2001; Jamal, Maier and Sunder, 2005c). Milberg et al. (1995) also suggest that lower levels of information privacy concern will be associated with countries with no privacy regulation.

Nigeria is known for its high level of cybercrime (Boniface, Michael and Victor, 2015; Ehimen and Bola, 2010), so many Nigerians are becoming aware of the dangers of putting credit/debit card details on just any website (Wolf Park and Digital Jewels, 2014). This has prompted many e-commerce websites to adopt the pay on delivery method (Chiejina and Olamide, 2014). This method provides peace of mind as no bank or card details can be compromised. There should be concern about the absence of any protection or resolution in the case of the website misusing personal data.

7.1.1.5 Illiteracy and Lack of awareness

Nigeria is one of the ten countries that contain the world's 775 million illiterate adults (CIA, 2015). In the context of understanding and using the Internet, this form of illiteracy could be regarded as digital illiteracy (Akanbi and Akanbi, 2012; Tayo, Thompson and Thompson, 2016). Many Nigerians are just beginning to understand what e-commerce is all about and thus they may not understand the concept of personal data protection in e-commerce. Nigeria

has also been identified as one of the fastest growing developing nations (Mcgroarty and Hinshaw, 2014), so more and more people are starting to use the Internet, but the vast majority of the Nigerian population that use the Internet are unaware of the dangers associated with it (National Information Technology Development Agency, 2013).

Data protection systems should create awareness about the danger of data misuse and what proper data protection policy is.

7.1.1.6 Reputation and a Lack of Interpersonal Trust

The rapid development of the nation's IT infrastructure (Bassey *et al.,* 2016) with the lack of regulation and enforcement has unfortunately, led to Nigeria becoming a centre for cybercrime that has given the country a bad reputation for Internet users both within and outside Nigeria. This reputation and the lack of trust it generates creates a need for data protection but, at the same time, inhibits the population from trusting any scheme that could be put in place to protect personal data (see Chapter 5).

7.2 Australian Industry-Dispute Benchmarks

The benchmarks developed by the Australian government for Industry-Based Customer Dispute Resolution Schemes form a suitable foundation to evaluate consumer dispute regulation (Australian Information Commissioner, 2013). Cavoukian and Crompton (2000) have used these benchmarks to evaluate the dispute resolution processes of three Web seals. These benchmarks cover the common content of international dispute resolution standards. The benchmarks according to the Australian benchmarks (Australian Information Commissioner, 2013) are structured around six main principles:

Benchmark 1 - Accessibility: "the scheme makes itself readily available to customers by promoting knowledge of its existence, being easy to use and having no cost barriers".

Benchmark 2 - Independence: "the decision-making process and administration of the scheme are independent from scheme members".

Benchmark 3 - Fairness: "the scheme produces decisions which are fair and seen to be fair by observing the principles of procedural fairness, by making decisions on the information before it and by having specific criteria upon which its decisions are based".

The key practices associated with Benchmark 3 specify that a dispute resolution scheme should be structured so that

1. The scheme's staff advise complainants of their right to access the legal system or other redress mechanisms at any stage if they are dissatisfied with any of the scheme's decisions or with the decision-maker's determination
2. Both parties can put their case to the decision-maker.
3. Both parties are told the arguments, and sufficient information to know the case of the other party
4. Both parties have the opportunity to rebut the arguments of, and information provided by, the other party.
5. Both parties are told of the reasons for any determination.
6. Complainants are advised of the reasons why a complaint is outside jurisdiction or is otherwise excluded.

Benchmark 4 — Accountability: "the scheme publicly accounts for its operations by

publishing its determinations and information about complaints and highlighting any systemic industry problems".

Benchmark 5 — Efficiency: "the scheme operates efficiently by keeping track of complaints, ensuring complaints are dealt with by the appropriate process or forum and regularly reviewing its performance".

Benchmark 6 — Effectiveness: "the scheme is effective by having appropriate and comprehensive terms of reference".

These benchmarks are used in the analysis of the government and self-regulation approaches in Sections 7.3 and 7.4.

7.3 Assessing Nigerian Potential Compliance with ICO Data Protection Guidelines

To enable adequate data protection mechanisms, there are some processes that any approach should perform: consumer dispute resolution, compliance monitoring and enforcement. This chapter examines these processes to determine what approach would be suitable for developing countries.

In nations where the data protection is regulated by the government, for example Austria, the Netherlands and the United Kingdom, the enforcement and compliance regulation is the responsibility of the government. As an example of a governmental, regulatory approach, the United Kingdom's Information Commissioner's Office (ICO) is examined in detail in the following:

7.3.1 Consumer Dispute Resolution

For a data protection approach to be effective there should be an appropriate method for customers to file complaints or concerns. It is also important that the complaints reach the appropriate personnel and are resolved promptly and suitably. If a customer discovers that their personal data managed by a Data Controller (online merchant) is inaccurate, or was processed illegally, the UK ICO's dispute resolution mechanism means the customer is entitled to (European Commision, 2013):

- "Ask the Data Controller for the data to be corrected, erased or blocked".
- "Demand that the Data Controller notify those who have already seen the incorrect data, unless this requires a disproportionate effort. A reasonable fee for providing access may sometimes be charged".
- "If the customer does not receive an adequate answer from the Data Controller, they can submit a complaint to the ICO".

The authority must investigate complaints and, if needed, briefly ban the data processing, which is the subject of the complaint. If the controlling authority finds that data protection law has been violated, it can demand the data be erased or destroyed and/or ban further processing (European Commision, 2013). An evaluation of the government regulatory system for use in Nigeria using the Australian Industry-Dispute Benchmarks gives the following (Australian Information Commissioner, 2013):

Benchmark 1 — Accessibility: For a system to work in Nigeria it has to be easily accessed and it should create awareness about data misuse and how to forward complaints to the right authority. This could help create awareness on the importance of personal data protection and what rights a data subject has. Popular web seals, such as TRUSTe,

require participants (data controllers) to display seals on their websites (TRUSTe, 2017a). The seal logo on the participating site links back to the seal's own website, which contains information about the available dispute resolution mechanisms. This system creates awareness about the dispute process.

Websites that conform to government regulations do not have an easily accessible system to provide customer dispute resolution, although some websites provide information to enable customers to file claims, ask questions and register complaints (Cavoukian and Crompton, 2000). This information is usually in the policy document, which in some cases is not easy to find (Cavoukian and Crompton, 2000).

The lack of awareness of Personal Identifiable Information (PII) privacy issues in Nigeria means that few people would know how to register a complaint and the lack of importance given to information privacy issues means that any resolution of issues would be difficult to enforce (see study results in Chapter 5).

Benchmark 2 — Independence: In self-regulating countries, if there is reason to believe that a site has not complied with its posted privacy commitments, the web seal owner, such as TRUSTe, may require an on-site compliance review by an independent third party, such as PriceWaterhouseCoopers (Cavoukian and Crompton, 2000). In the UK, all dispute resolution processes are handled solely by the Information Commission Office, although they occasionally work closely with other UK regulators where there is a shared interest in regulatory action and data protection authorities in other countries (Information Commisioner's Office, 2013).

With Nigeria dealing with economic issues such as corruption, electricity shortages, disputing data protection issues properly without external help may not be a priority (Uma and Eboh, 2013).

Benchmark 3 — Fairness: The United Kingdom's Information Commissioner's Office seems to practice fair dispute resolution. According to the data protection Regulatory Action Policy document, it is indicated that they practice five principles of good regulation: transparency, accountability, proportionality, consistency and targeting (Information Commisioner's Office, 2013) The political history of Nigeria means that people will be reluctant to embrace transparency and the general lack of trust would mean that even if transparency was achieved it might not be trusted.

Benchmark 4 — Accountability: The Information Commissioner's Office posts dispute resolution decisions and complaint statistics, with brief summaries of the issues raised on its website. This includes detailed information on, monetary penalty, decision notices, trends, undertakings, enforcement notices and prosecutions of various organisations (Infomation Commisioner's Office, 2017). They also have a news and event session with stories about high profile online privacy incidents. With Nigeria's political history, it is clear that there would be a reluctance to be so open, and even if this openness were achieved the lack of interest in privacy issues would mean it would be unlikely to achieve the same impact as in the UK. This benchmark insinuates transparency but Nigeria is known for its government's lack of transparency (Wolf Park and Digital Jewels, 2014; Transparency International, 2015). Even if the government is fully responsible for posting dispute resolution decisions and complaint statistics, it is likely that customers will not fully trust it (also see Chapter 5 study results).

Benchmark 5 — Efficiency: The Information Commissioner's Office publishes a complaints performance document on its website. This shows the annual casework created and finished. They also show how long it takes for them to finish casework (Information Commissioner officer, 2014).

Benchmark 6 — Effectiveness: The Information Commissioner's Office has detailed terms of reference. However, in Nigeria, the lack of appropriate legislation and the low priority to be given such legislation means that an equivalent of the UK's ICO could not be as effective. Table 7.1 summarises the evaluation discussed.

Table 7.1: Evaluation of ICO's dispute resolution practices

Benchmarks	**ICO's Dispute Resolution practices**	**Nigerian Factor**
Accessibility	Not easily accessible dispute resolution scheme Usually located at a not easily accessible privacy policy	There is a Lack of Personal Identifiable Information misuse awareness and a perception of a lack of Personal Identifiable Information importance
Independence	Dispute resolution processes are handled solely by the ICO	Current economic issues may prevent proper sole dispute resolutions
Fairness	The ICO practices fair dispute resolution practices	There may not be fair practices due to Government history and priorities
Accountability	The ICO posts dispute resolution decisions complaint statistics, and brief summaries of the issues raised on its website	The government is known for its lack of transparency
Efficiency	The ICO publishes a complaints performance document on its website	Economic issues may prevent effectiveness in this regard
Effectiveness	The ICO has detailed terms of reference	A lack of any legislation could hinder effectiveness

7.3.2 Compliance Monitoring and Enforcement

In order to ensure good privacy practices from organisations, rigorous compliance and enforcement functions must be in place (Rudraswamy and Vance, 2001). Strong compliance

and enforcement processes enhance the privacy principles and dispute resolution mechanisms by strengthening the consumer's trust. Compliance monitoring refers to those processes designed to ensure that the claims made by the data controllers on their websites are adequate, and that they are complying with the claims they have made to their customers relating to information protection, transaction integrity, business and information practices. Enforcement comes into play when the compliance process has gathered sufficient evidence that a website has been unable to adhere to the claims made to its customers (Cavoukian and Crompton, 2000).

Caukovian and Crompton (2000) evaluated the self-regulation system elements of the compliance and enforcement functions for registration, standards, objectives, processes, and enforcement. However, for a government-regulated system, only registration, processes and enforcement are of interest. The standards and objective elements describe the aims and objectives and not the practical aspects of compliance monitoring and enforcement.

Registration: Web seal organisations, for example TRUSTe, will initially review the website for adherence to TRUSTe programme principles and privacy statement requirements and also require the data controller to complete a self-assessment questionnaire (Markert, 2002). In the UK, the Data Protection Act of 1998 requires every data controller who processes personal information to register with the Information Commissioner's Office (Information Commissioner officer, 2014). The ICO provides guidelines and a checklist that data controllers can use to check how they are doing. The registration process, if the ICO's approach is adopted in Nigeria, could possibly work, but this, in itself, is not effective unless the ICO itself is an effective institution.

Processes: In the United Kingdom, the ICO conducts audits for public and private companies, public authorities and government departments. These audits are voluntary

and are usually requested (Information Commisioner's office, 2014). Although it is most suited to larger organisations with an understanding of the basics of compliance, the ICO also performs advisory visits for small to medium sized businesses. The visit is to give practical advice to organisations on how to improve data protection practice and also review what is carried out in practice (Information Commissioner's Office, 2015). In addition, the ICO encourages a self-assessment programme, which is aimed at promoting good personal data protection practice within sectors where there are a lot of smaller organisations or public authorities (Information Commissioner Officer, 2014). Most compulsory audits are initiated by public complaints.

In Nigeria, it is unlikely that there will be sufficient interest in privacy issues for website owners to regularly request an audit or a self-assessment programme. Compulsory audits may work in Nigeria, but only if the legislation was in place to make sure it happened. This is not likely to be a government priority in the immediate future.

Enforcement: The ICO investigates complaints and may temporarily ban any data processing, which is the subject of a complaint. If the ICO finds that data protection law has been violated, it can order the data be erased or destroyed and/or it can ban further processing. If the data controller refuses to make acceptable corrections or the breach is found serious, the ICO can issue a monetary penalty (European commision, 2013). Clearly, there would be a lot of legislation necessary for such a scheme to be implemented in Nigeria, but this is unlikely in the near future. However, without this, the ICO cannot be effective. Table 7.2 summarises the evaluation.

Table 7.2: Evaluation of the ICO's compliance monitoring and enforcement practices

	ICO Practices	Nigerian Factors
Registration	Every website that processes personal information to register with the ICO	This system can only work with an effective ICO type institution
Processes	The ICO conduct voluntary advisory visits and audits	Little interest in PII security means website owners are unlikely to request audits
Enforcement	The ICO can temporary or permanently ban processing	The lack of any enacted legislation may prevent proper implementation

7.4 Assessing Nigerian Potential Compliance with TRUSTe's Data Protection Guidelines

This section examines TRUSTe's data protection approach with a similar approach used with the government's data protection approach. TRUSTe is an independent, non-profit privacy organization dedicated to building users' trust and confidence on the Internet (see Section 2.2).

7.4.1 Consumer Dispute Resolution

For a data protection approach to be effective there should be an appropriate method for customers to file complaints or concerns. It is also important that the complaints reach the appropriate personnel and are resolved promptly and suitably. If a customer discovers that their personal data managed by a Data Controller (online merchant) is inaccurate, or was processed illegally, TRUSTe's dispute resolution mechanism means they are entitled to:

- Confirm that the Website in question is a TRUSTe client.
- Verify that the complaint is a privacy matter relating to a TRUSTe client Website.

- Contact the TRUSTe client Website first

If the TRUSTe member does not resolve the complaint appropriately, TRUSTe will review to check the complaint's eligibility and mediate a solution (TRUSTe, 2017b). Penalties that TRUSTe could impose on the violator are suspension and even termination of their programme and/or notifying government authorities such as the FTC (Federal Trade Commission) if the violator still fails to comply (TRUSTe, 2017b).

Evaluating TRUSTe's approach for application in Nigeria using the Australian Industry-Dispute Benchmarks gives:

Benchmark 1 — Accessibility: For a system to work in Nigeria it has to be easily accessed and it should create awareness about data misuse and how to forward complaints to the right authority. TRUSTe requires participants (data controllers) to display seals on their websites. The seal logo on the participating site links back to the seal's own website, which contains information about the available dispute resolution mechanisms (TRUSTe, 2017b). This system creates awareness of the dispute process. Details of TRUSTe's complaints mechanisms are accessible from their official website and hence from their seal logo's link. This also verifies that the website is really a TRUSTe participant.

Adopting a data protection system with a similar accessible and transparent approach could help create awareness about data misuse and how to complain to the right authority. This could help create awareness on the importance of personal data protection and what rights a data subject has.

Benchmark 2 — Independence: If there is reason to believe that a site has not complied with its posted privacy commitments, TRUSTe may require an on-site compliance

review by an independent third party, such as PriceWaterhouseCoopers (Cavoukian and Crompton, 2000).

With Nigeria dealing with economic issues such as corruption, electricity shortages, and so on, disputing data protection issues properly without external help may not be a priority. Therefore, sourcing external help to help solve disputes rather than relying solely on the government may be a good data protection system to adopt.

Benchmark 3 — Fairness: TRUSTe seems to practice fair dispute resolution. They provide for each party to receive information about the arguments of the other, advise complainants of other avenues if any are available, and to be told the reasons for TRUSTe's decision. This substantially meets the requirements of benchmark 3 (TRUSTe, 2013).

The political history of Nigeria and the lack of trust in the government could mean that people will be reluctant to embrace transparency and the general lack of trust would mean that even if transparency was achieved it may not be trusted. This may not be the case if handled by a third party organization, particularly if that organisation already has a well-established, good reputation.

Benchmark 4 — Accountability: TRUSTe publishes a generic annual transparency report that shows how many complaints were raised and how many were resolved (TRUSTe, 2013). Due to the lack of trust in Government, adopting a trusted non-government organisation like TRUSTe could be a better approach.

Benchmark 5 — Efficiency: TRUSTe publish a transparency report that shows details about the annual complaint performance. This shows the annual casework created and finished. They also show how long it takes for them to finish casework (TRUSTe,

2017a). The pressures on a developing country government are such that data privacy is unlikely to be given the priority to ensure its efficiency. It may be a better option to delegate this aspect to a third party organization such as TRUSTe.

Benchmark 6 — Effectiveness: TRUSTe has detailed terms of reference (TRUSTe, 2017a). However, in Nigeria, the lack of appropriate legislation and the low priority given for any new legislation means it may not be effective. Assigning data protection to a non-government organisation could mean an effective term of reference. Table 7.3 summarises the discussions above.

Table 7.3: Evaluation of TRUSTE's dispute resolution practices

Benchmarks	**TRUSTe's Dispute Resolution Practices**	**Nigerian Factor**
Accessibility	Easily accessible seal logo that redirects to dispute resolution information	Adopting similar approach could increase awareness and PII importance.
Independence	May require an on-site compliance review by an independent third party	Relying less on the government may be a way of dealing with the economic priority factor
Fairness	TRUSTe seems to practice fair dispute resolution.	Due to lack of trust and opaque government, people may trust TRUSTe's approach more than that of their government.
Accountability	An annual transparency report shows how many complaints were raised and how many were resolved	The government is known for its lack of transparency. Reports by a non-government body are more likely to be trusted.
Efficiency	Transparency report that gives details of annual complaint performance	It may be a better option to delegate transparency reports to a third party organisation.
Effectiveness	TRUSTe has detailed terms of reference.	Assigning data protection to a non-government organisation could become an effective term of reference.

7.4.2 Compliance Monitoring and Enforcement

TRUSTe and the ICO have similar elements in terms of registration, compliance monitoring and enforcement elements. However, unlike the ICO, the registration and compliance monitoring for TRUSTe are involuntary.

Registration: TRUSTe will initially review the website for adherence to TRUSTe programme principles and privacy statement requirements and also require the data controller to complete a self-assessment questionnaire. This system provides information about the participant's privacy practices, which will determine if the seal will be issued or not (TRUSTe, 2017b). With the absence of effective data protection legislation, implementing an approach similar to that of TRUSTe may be successful.

Processes: Unlike the United Kingdom ICO that conducts requested voluntary audits and advisory visits (Information Commisioner's office, 2014), TRUSTe representatives periodically review the website to ensure compliance with posted privacy practices and program requirements and to check for changes to the privacy statement (TRUSTe, 2017b).

TRUSTe regularly "seeds" websites, which is the process of tracking unique identifiers in a site's database. Unique user information is submitted and results monitored to ensure that the website is practicing information collection and uses practices that are consistent with its stated policies (TRUSTe, 2017a). TRUSTe also relies on online users to report violations of posted privacy policies, misuse of the TRUSTe seal, or specific privacy concerns pertaining to a website (TRUSTe, 2017b; TRUSTe, 2017a).

Due to lack of a legislation to conduct and monitor compulsory audits, implementing the self-regulatory approach with the help of web assurance organisations to perform compulsory audits could be a more successful approach.

Enforcement: Depending on the severity of the breach, the investigation could result in an on-site compliance review by a CPA (Certified Public Accountant) firm and/or withdrawal of the site's seal/license. After TRUSTe has exhausted all escalation efforts, extreme violations are referred to the appropriate law authority (TRUSTe, 2017b; TRUSTe, 2017a). This approach tries to resolve enforcement issues without involving the government except in extreme situations. With the present unlikeliness of data protection legislation in Nigeria, a non-government body such as TRUSTe could be responsible for issuing appropriate penalties. Table 7.4 summarises the evaluation.

Table 7.4: Evaluation of Truste's compliance monitoring and enforcement practices

	TRUSTe's Practices	**Nigerian factor**
Registration	Reviews the website and also requires the data controller to complete a self-assessment questionnaire	This may be a good alternative in the absence of an ICO type organisation
Processes	Periodically reviews the Web site to ensure compliance	Compulsory audits may be a good alternative as there is little interest in PII security
Enforcement	Conducts onsite compliance review depending on severity	A non-governmental body responsible for issuing appropriate penalties could be a viable alternative in the absence of any legislation

7.5 Conclusions

The Information Commissioner's Office (ICO) provides guidelines and voluntary audits to ensure compliance. A compulsory audit usually takes place if a complaint is filed or if a public organisation is involved. If a customer has no idea of their rights as a data subject or the responsibility of a data controller, they may not file any complaints and the data controller's practices may go unchecked. If, when a complaint is filed, the legislation needs to be in place for an office equivalent to the UK's ICO to be able to effectively act against the website owner.

Although it is stated that all data controllers must register with the ICO, there was no mention on how to enforce this law. In Nigeria, it is possible that many data controllers would not see the need to register and, as long as there are no complaints, they would have no problems. In Nigeria's case, where there may be little awareness of personal information misuse and data protection rights, the voluntary system of the ICO may not be a suitable approach. The governmental regulatory approach through an institution equivalent to the UK's ICO is unlikely to be effective in a country such as Nigeria where government priorities will mean that such an office would be unlikely to be given the resources and legislation it needs to be effective. Additionally, the country's economic situation and traditions mean that most people are either unaware of data privacy issues or are not sufficiently interested to take action.

TRUSTe's alternative approach ensures that the data controllers are adhering to their requirements by constant compulsory audits and self-assessment questionnaires, unlike the United Kingdom's ICO that just provides guidelines and voluntary audits to ensure compliance. In a case where the customer is oblivious to their rights, TRUSTe can still monitor the data controller's compliance and ensure good privacy practices.

As registering with a web assurance organisation, such as TRUSTe, is not compulsory in practicing countries, many data controllers in Nigeria would not register and customers may then not have any means of complaint. In Nigeria's case where there may be little awareness on personal information misuse and data protection rights, the voluntary registration process of self-regulation may not be a suitable approach.

Any approach that may work in Nigeria should have a dispute resolution system that is very easy to access and understand and have little or no government involvement, it should also have a strict compliance monitoring system. This study has shown that the self-regulatory approach is likely to be effective in Nigeria, although some of the aspects of this approach such as the voluntary registration may seem ineffective. However, if voluntary registration became widespread and customers became more aware of the meaning of Web seals, then public and commercial pressure would encourage organisations to take up a voluntary, self-regulatory approach.

Chapter 8 discusses the findings of this research and makes recommendations based on them. The chapter also evaluates the recommendations via surveys.

Chapter 8: Findings and Recommendations

Studies confirm that both technological and non-technical solutions to data protection and privacy cannot be relied on without putting the human factor into consideration, and awareness training is considered an effective method for reducing cybercrime (Cox, Connolly and Currall, 2001; Desman, 2003). Although this research supports self-regulation, there are no guarantees about online businesses' actually privacy practices. Therefore, the focus of this research is on improving privacy and data protection by enhancing Internet security awareness and by proposing recommendations for relevant stakeholders in Internet security. A security and privacy awareness programme would be considered effective if it is capable of establishing for participants the appropriate knowledge on self-protection techniques and it influences the attitude and behaviour of the participants to make positive changes in their security culture (Kritzinger and von Solms, 2010; Woon, Tan and Low, 2005). In this research, the focus is improving security culture by promoting Internet security awareness as part of an overall framework.

This chapter describes the framework that consists of a set of recommendations for the Nigerian government, recommendations for organisation officials responsible for ensuring the protection of personal information, and an effective awareness programme to reduce the problem of privacy and data protection in developing countries.

This chapter defines the recommendations part of the framework; the awareness programme is discussed in detail in Chapters 9 and 10. These recommendations have been evaluated by relevant experts to identify their potential for reducing privacy and data protection issues in developing countries, using Nigeria as a case study.

8.1 Findings

The main contribution of this research is to propose a tailored effective framework to reduce the Internet privacy and data protection issue, which could be a threat to the adoption and penetration of e-commerce in Nigeria. This was developed using findings from previous chapters (Chapters 5, 6 and 7). A summary of the outcomes of each chapter is given in table 8.1.

All of the findings have clearly demonstrated that Nigerian Internet users are vulnerable when online due to the general lack of awareness and websites' poor privacy practices. There are also various factors that could affect the data protection and privacy practices of a country with many country specific factors behind Nigeria's lack of an effective solution. Consequently, there is a need for an effective way to regulate the websites' practices and also improve Internet users' awareness. Sets of recommendations were therefore identified for relevant stakeholders in Section 8.2.

Table 8.1: Main findings from research

Chapters	**Main findings**
E-commerce, Internet and Internet Privacy in Nigeria (Chapter 5)	Even though Internet access has yet to reach more than 50% of Africans, the continent's connectivity levels are nonetheless growing at a rapid rate according to data compiled by Internet Live Stats (2015). Cybercrime is more prevalent in Nigeria due to the population size, the push towards a cashless society, relatively high Internet penetration, a lack of adequate security controls, and weak governance. It was also discovered that many Nigerians are unskilled, which could pose a significant risk to the state of Internet security in the country. The lack of a data protection laws was identified as one of the major problems in Nigerian e-commerce privacy and data protection.

	A study was undertaken to understand the attitudes of Nigerians about privacy through a written survey and interviews. The results show that a majority have accepted the disclosure of personal information is necessary for e-commerce but appear to be minimally concerned about providing information unless financial information is concerned. While there is high Internet penetration in Nigeria, the Internet security culture is lacking. Nigerians are largely unaware of self-protection techniques and they show little concern for security issues. In addition, the current awareness initiatives may be ineffective in combating these problems. This could pose a major problem in the development of e-commerce due to Nigeria's high cybercrime rate
Analysis of Data protection and privacy practices in Nigeria (Chapter 6)	65 websites' policy content were analysed to gather information about the websites' policy practices. Also a web crawler, a tool designed to record and analyse online data practices was used to gather data from these websites. It was discovered that although the majority of the websites make use of cookies many fail to disclose information about this practice. Overall most of the websites fail to adequately fulfil the general guidelines for good privacy practices and significant improvements are needed in this regard.
Different data protection approaches (Chapter 7)	In Chapter 7, It was discovered that a nation's socio-cultural and economic factors could determine a nation's view of Internet privacy and data protection and the approaches adopted. This could affect the Internet security culture of the country, which could either hinder or promote e-commerce and Internet adoption. The government and self-regulation approaches of developed nations were evaluated in detail to determine why they may not be effective in developing nations. The United Kingdom and United States were used as case studies. It was concluded that any approach that could be adopted in Nigeria would need to have less government involvement. Furthermore, the solution would need to improve Internet users' awareness before it can be effective.

8.2 Recommendations

This section describes the recommendations made for relevant stakeholders based on the findings in previous chapters. The relevant stakeholders are the Nigerian government and organisations directly and indirectly responsible for ensuring personal information privacy and Internet security, such as financial institutions and e-commerce businesses.

8.2.1 Recommendations for the Nigerian Government

Findings from previous chapters (Chapter 5, 6 and 7) show clearly the need for a solution to the data protection and privacy issues and also show the need to enhance people's awareness of these issues in Nigeria. Although there are some existing awareness programmes, the most common awareness programmes are web based. These programmes are, in most cases, not easy to find and, with the level of illiteracy among Nigerian home users, they may not have the skills and knowledge to find these programmes. It was also discovered that due to the cultural and environmental factors in Nigeria, it might be more effective to delegate Internet privacy and data protection to relevant organisations, though the government also has a part to play.

Organisations, such as the banks, can benefit from their customers being aware of cybercrime issues as this can reduce financial related cybercrime, which could reduce the banks' vulnerability to significant financial, regulatory, and reputational risk. However, rather than just waiting for affected organisations to take action, it may be more effective if the government could provide incentives for the relevant organisations to provide awareness initiatives for their customers.

The literature review (Obutte, 2014; Perchstone & Graeys, 2016) has revealed that there are no explicit data protection laws in Nigeria. Although there are draft guidelines on Data

Protection, published by the National Information Technology Development Agency, they have little or no legislative authority and are, therefore, ineffective. The recommendations of this research are:

1. While the Nigerian government may not be currently in the position to enact any legislation, it is recommended that a legislative body to make the draft effective and equivalent to those in developed countries.
2. It is also recommended that extensive research should be funded on e-commerce; e-crime and cyber-security and their effect on the Nigerian economy. The research should also focus on identifying factors, which affect Internet security and privacy in Nigeria, and on investigating how to defend against cyber issues taking into account the factors that affect Nigeria.

8.2.2 Recommendations for Organisations Responsible for Ensuring Internet Privacy and Security

Some of the organisations involved in e-commerce are the banks who usually handle payments and ensure the security of financial data, and the Internet service providers and/or telecommunication companies who provide Internet services for Internet users. There needs to be recognition that technological solutions and privacy policies alone cannot be relied on to protect Internet users and, therefore, awareness will act as another level of defence to ensure the effectiveness of technological solutions and policies. Therefore, it is recommended that the e-commerce organisations develop effective awareness programmes for their customers. Due to the generally unskilled population, security culture and the low perceived importance of personal information privacy, cyber-security awareness needs be actively promoted or awareness programmes will simply be ignored. This study agrees that, although

awareness programmes accessible in Nigeria already exist, they are, in most cases, not easy to find and, with the level of digital illiteracy and lack of interest, Nigerian HUs may not have the skills and knowledge to find these programmes. Furthermore, a security-illiterate person will not even know of the need to search for these online awareness programmes, particularly as personal information security has been found not be an overly important issue for Nigerians. The recommendations of the research on security and privacy awareness are, therefore:

1. It is recommended that the awareness programme should expose users to awareness tools by implementing contextual training (see Chapter 2, Section 2.5.3) to prepare them for the possible risks when accessing the Internet. Contextual training is where the user is automatically prompted to do training that is immediately available and relevant to the action that the user is currently undertaking (see Chapter 9 for more information on a recommended awareness programme). The Internet users would, therefore, immediately be able to have more information about security threats when faced with a potential risk; this could be described as promoting awareness in that the user would have no choice but to see the training is available, but they would not be obliged to follow it. Private organisations such as Internet service providers, telecommunication companies and financial institutions could provide this service.
2. It is also recommended that Nigerian online business owners should employ independent, approved and trusted third party organisations similar to TRUSTe to audit and monitor websites security and privacy practices. The trusted organisation would ensure the websites practices are appropriate and the level of awareness of their employees is adequate. Nigerian banks hold a significant part to play in e-commerce as they ensure the financial protection of customers when performing transactions online. It has been discovered that financial information is very important to Nigerian

Internet users and the banks are held in high regard on this issue. If the practices of a website are endorsed by the banks, it could improve the trust Nigerians have for the site and, to get this endorsement may mean a site would need to improve its practices.

8.3 Evaluation of Recommendations

To evaluate the proposed recommendations, interviews and questionnaires were utilised. Five experts were asked for their opinions in semi-structured interviews. Questions were asked about the current practices, the recommendations were presented, and then face-to-face individual discussions were held to evaluate the recommendations (see appendix B). All the selected experts are operating in Nigeria and were selected based on their job titles, responsibilities and their involvement in Internet security and e-commerce (banks, Internet service providers and government). The experts were referrals and recommendations from the researcher's previous professional contacts.

A covering letter was sent them describing the aim of the study and reason for the Interviews. The emails were sent to six Interviewees, however due to time constraints, just five interviews were conducted. The interviews were transcribed immediately after each interview and written up while the interview was still fresh in the mind of the researcher. This enabled the researcher to clarify the information acquired and to decide what information was required in the writing up. The notetaking method of recording the interview was chosen due to the researcher's previous experience that Nigerians are generally not happy with audio recordings of interviews. The five experts were:

- A CEO of an e-commerce business: The participant interviewed is the founder of an up and coming e-commerce website in Nigeria. He is also involved in the IT management department of the company. It was useful to get his opinion due to his

in-depth knowledge of the e-commerce background in Nigeria since he has been able to successfully create and run an e-commerce business in Nigeria despite the obstacles involved.

- An IT management employee of an e-commerce business: The participant interviewed works in the IT department and handles IT related issues such as monitoring the servers, the website's security and so on. He provided insight on how security issues are managed and the limitations that comes with managing a secure website in Nigeria.
- An IT specialist of a commercial bank: The participant interviewed provided insight on how involved the banks are in providing payment services to e-commerce websites. This was important because one of the main recommendations of this study is for private institutions such as the banks to provide awareness programmes. It was important to get their views on the probability of implementing the recommendations.
- Two government officials at the Ministry of Information Technology: The officials interviewed work at the government office based in Lagos and are usually involved in any nationwide IT related initiatives. It was useful to verify the government's involvement in promoting Internet security and understand their views on the recommendations to involve more private organisations in the issue.

The discussions were based on the following questions:

1. What is the current privacy and data protection situation in their respective industries?
2. Are the recommendations useful and do you think they will help in reducing the privacy and data protection risk in Nigeria?
3. Are they viable and applicable to Nigeria?

4. Are there any limitations that might be experienced if they were implemented?

5. Do you have any further suggestions or comments?

8.3.1 Recommendations for Organisations Responsible for Ensuring Internet Privacy and Security

Generally, the experts believed that the recommendations (see Section 8.2.2) were potentially effective and if implemented successfully, they would certainly help in reducing the privacy risk in Nigeria.

The interviewed CEO of an e-commerce business stated that their website is hosted in the United States because of a lack of resources in Nigeria, such as electricity and bandwidth, which is mainly due to the Nigerian government's inadequacies. He indicated that the recommendations would be potentially effective because most of the financial aspects (such as protection credit/debit card and financial dispute handling) of the company's transactions are carried out by the bank and involving them in regulating data protection services could be possible.

The IT management employee of a similar retail online business, founded in 2012, also stated that the business's website is hosted in the United States and the major website security is handled over there. A lack of electricity and insufficient bandwidth were, again, cited as the main reason for not hosting in Nigeria, with poor Internet security as an additional reason. He also stated that he is sure that some sort of privacy policy exists in Nigeria, but he is not sure if the policies are operative or enforced as his business implements good practice in their security systems for reputation and company policy reasons. Their bank also provides payment security and handles customer disputes, which are usually financial in nature. He agreed that fully involving a third party organisation, such as a bank may be beneficial,

however, he doubted if excluding the government entirely would be a good idea. This was regarded as a limitation to the recommendations.

The IT specialist of a leading commercial bank in Nigeria, which provides services specific to e-commerce websites, was interviewed about the services the bank provides for e-commerce websites and how they ensure compliance with good security and data protection practices. The most common and important service the bank provides is the payment gateway platform. This platform plugs in seamlessly to existing websites of merchants and acts as a bridge between the customer's website and financial institutions (banks). The bank has complete control over any financial transaction performed on the website, this means that the bank handles all security issues. Although they do not explicitly require the websites to follow any practices, the bank requires intending merchants to:

- Be a customer of the bank
- Be under the right category of customer (must be a business/merchant customer)
- Have an eligible business

Most disputes handled are usually financial in nature and have usually been through a rigorous investigation and validation processes. They agree that getting fully involved in the data protection practices might be an effective idea and potentially implementable. However, one of the concerns was how efficient the banks would be in providing this service without an incentive or government involvement.

8.3.2 Recommendation for Nigeria Government

In order to evaluate the recommendations made for the government, the two government officials were interviewed. Both of them were employees at the Ministry of Information Technology.

They both stated that there is not any current legislation similar to the ones being implemented in the United Kingdom. However, a cybercrime bill was being drafted and would soon be signed into law. They both agreed that, although the bill imposes certain security obligations on organisations operating computer systems and networks, it does not sufficiently address data protection. It was also generally agreed that the current economic situation in Nigeria might be the reason why they are lagging behind on this issue.

Generally, they agreed that the recommendations (see Section 8.2.1) were applicable to the current situation in Nigeria and it is a necessary step to address the cybercrime issue in Nigeria. Concerning the second recommendation, it was stated that research on cyber-security is already underway and some initiatives are being considered.

Finally, one the officials highlighted the need to involve other parties such as non-governmental organisations (NGOs) in organising awareness seminars and that they should engage in more research which could further motivate the government to implement the proposed recommendations.

8.4 Conclusions

This chapter presented the recommendations for the Nigerian government and for the organisations responsible for ensuring the privacy and security of Nigerian Internet users. The recommendations were based on findings from the research carried out during the study. Sample relevant experts evaluated the proposed recommendations (see Section 8.3). They concluded that the recommendations were potentially effective if implemented successfully and could help in reducing the privacy and data protection risk in Nigeria. However, there was a general advocacy for the Nigerian government to be more involved in privacy issues in Nigeria, rather than solely relying on the industries.

The experts thought that the recommendation to enact legislation and to develop a legislative body was relevant to the current situation in Nigeria and it would be useful to enact a proper legislative body. However, it was noted that the recommendations would be much more achievable if the government collaborates with non-governmental organisations.

Concerning the recommendations for private institutions and Internet users responsible for their Internet privacy and security, the experts stated that the recommendations would be a good idea considering the fact that the government is currently ineffective. Based on the interviews, it was evident that privacy and security practiced in their websites complies only with their companies' own guidelines and those of their banks with little or no government involvement in any standards or practices.

Although the study also recommends that an awareness programme be implemented (see Section 8.2.2), this chapter did not focus on the evaluation of the awareness programme, as it is the major aspect of the framework. The next chapter (Chapter 9) comprehensively describes the awareness programme and Chapter 10 describes the development and evaluation of the programme.

Chapter 9: Promoting Cyber-security Awareness through Contextual Training linked to Security Warnings

In Chapter 8, it was recommended that relevant organisations should educate Internet users and customers on cyber-risks via an awareness programme. Furthermore, it was recommended that the awareness programme be actively promoted. This is based on the finding that, due to the level of illiteracy and lack of interest, many Internet users may not have the skills and knowledge to find and follow a generic awareness programme. This chapter primarily focuses on Nigerian Internet home-users and their lack of Internet security awareness and suggests the need for promoting Internet security awareness in Nigeria. It describes the awareness programme in detail and proposes methods for developing and implementing the programme.

Various studies have stated that privacy security is one of the main concerns for successful e-commerce implementation. Studies also claim that it is more effective to address the social aspects of Internet security in addition to the technological aspects (see Chapter 2, Section 2.5.4).

Chapter 5 discusses the security concern about e-commerce in Nigeria, due to a general lack of awareness of cyber threats and an increase of online retail stores and e-commerce activity. A home user is a citizen of any age and technical knowledge who accesses the Internet for personal use anywhere outside their work environments. Home users can be further divided into students, parents and educators, young professionals and older citizens. The awareness programme described will focus mainly on Nigerian home users; this is because non-home users could have compulsory awareness training within their work environment unlike home-users who make use of the Internet without any training (Kritzinger and von Solms, 2010).

Firstly, this chapter discusses current awareness initiatives in Nigeria and other countries in order to evaluate the applicability and effectiveness of these approaches. It then suggests and discusses enforcing Internet security awareness and identifies the advantages of the approach. The literature review (Chapter 2, Section 2.5.3) discusses various awareness-training methods such as passive computer-based and web-based training and contextual training. This chapter discusses integrating these training methods into the awareness programme. Finally, the chapter proposes methods of developing and implementing the programme.

9.1 Internet Security Awareness Initiatives

Although the Internet offers an endless list of services and opportunities, it is also accompanied by many risks and dangers, of which many Internet users may not be aware. Therefore, various countries have developed and implemented cyber-security awareness measures to counter this. However, Nigeria is currently definitely lacking in this regard, as there are currently, few government-led and sponsored security awareness initiatives. This section describes initiatives developed in other developing countries as well as Nigeria.

9.1.1 Developed Countries

To explore the way other countries, promote Internet security awareness, Kortjan and Von Solms, (2014) conducted a comparative analysis of developed countries. The countries analysed were the United States of America (US) and the United Kingdom (UK). These countries were chosen because they have national cyber-security strategies and they are listed in the Organization for Economic Cooperation and Development (OECD) (Kortjan and Von Solms, 2014). The OECD is relevant because they provide guidelines for online practices.

In the US, the goal of cyber-security awareness and education is to raise the level of awareness in the nation on the risks of cyberspace, and how to avoid these risks (National Initiative for Cybersecurity Education, 2015). The National Initiative for Cyber-security Education (NICE) is dedicated to cyber-security awareness and education. NICE was created from a combination of governmental departments. The NICE Strategic Plan uses campaigns, such as "Stop. Think. Connect" to equip the US public with the necessary knowledge and skills. The "Stop. Think. Connect" website provides Internet security tips for different types of US citizens and campaigns for different Internet security issues.

In the UK, the goal is to support individuals and businesses by informing and educating them on the issue of cyber-security (UK Government Cabinet Office, 2013). Cyber-security awareness and education have been delegated to an external organisation, "Get Safe Online". The UK "Get Safe Online" website also has similar campaigns and tips tailored for different UK audiences. In both the US and UK, it is obvious that the cyber-security awareness and education goal is run by the government or delegated to one or more departments or organisations to carry out.

9.1.2 Nigeria

Even though Internet access is yet to reach more than 50% of Africans, the continent's connectivity levels are nonetheless growing at a rapid rate. As mentioned in Chapter 3, data compiled by Internet Live stats (2015) show that the African country with the highest number of Internet users in 2014 was Nigeria with 75.7 million users. The high figures of Internet usage and penetration in Africa have led to some awareness of cyber-security threats and, as a result, countries have started to take steps towards improving their respective security stance. However, this section will outline how African countries, and Nigeria in particular, are still lagging behind other countries in terms of establishing legislation to deal with Internet

security and creating initiatives to develop awareness about the Internet. It will also outline Nigeria's unique factors that will justify the awareness programme recommended (see Chapter 7), which is different from the generic approach used in most countries. Most countries make use of online awareness websites and campaigns, which provide information on different Internet security issues, but training on these topics is neither enforced nor promoted to any significant extent.

Based on the results from the study on the public's understanding and knowledge of data protection and privacy in Nigeria described in Chapter 5, it is shown that there are concerns about Internet privacy and security, and the awareness about how to prevent issues is relatively lacking. This means that although the survey participants imply concern for security of their personal information, the lack of security awareness and knowledge shows there is actually no concern for these issues.

9.1.2 1 Current Initiatives in Nigeria

CSEAN (Cyber-security Experts Association of Nigeria) is a non- profit organisation whose aim is to expand the Nigerians' knowledge, awareness and understanding of the issues around cybercrime and Internet security, mainly through workshops and seminars (CSEAN, 2015). The CSEAN partners with "Stop. Think. Connect" a global cyber-security awareness campaign initiated in the US. CSEAN will start the "Stop. Think. Connect" campaign in all tertiary institutions in Nigeria in the form of seminars(Oludare, 2015). ngCert (Nigerian Computer Emergency Response Team) is the national computer emergency response team that was created as a result of the 2015 Nigerian cybercrime bill (ngCert, 2014). Their website provides information on how to report a cybercrime incident. Most importantly, it provides some links to external advice and alerts on Internet security. However, CSEAN mainly uses seminars and events to improve general awareness in Nigeria. Seminars are not

easily accessible to many people as they are location-restricted and usually costly to attend. The ngCert website fails to provide adequate awareness information on safe Internet practices as compared to equivalent awareness websites in other countries. For example, in an equivalent UK website, the ICO (Information Commissioner's Office) provides advice on personal information protection and general Internet security (Information Commisioner's Office, 2016).

9.2 Enforcing Internet Security Awareness

With growing numbers of Nigerian home users accessing the Internet, the big problem and worry is that in many cases such users are not information security aware, and are therefore potentially exposing themselves to attack (Wolf Park and Digital Jewels, 2014). Kritzinger and von Solms (2010) suggested a way to force home users to gain necessary awareness before gaining access to the Internet. They pointed out that, unlike non-home users (NHUs), who are probably exposed to compulsory security awareness courses and are governed by corporate policies, procedures and guidelines when accessing the Internet, home users (HUs) are not necessarily forced to obtain information security knowledge in any form. If HUs lack the proper information security awareness knowledge, they will also not understand and/or be aware of the cyber risks (Furnell, Tsaganidi and Phippen, 2008). Figure 9.1 describes Kritzinger and von Solms's suggestion for enforced awareness before going online. It depicts a scalable model where a user can start with introductory material and then move on to more advanced content. The Internet user has to complete the awareness programme before they can access the Internet. The first component of the model is the awareness component, called the E-Awareness Portal (E-AP). The E-Awareness Portal provides the information security awareness content.

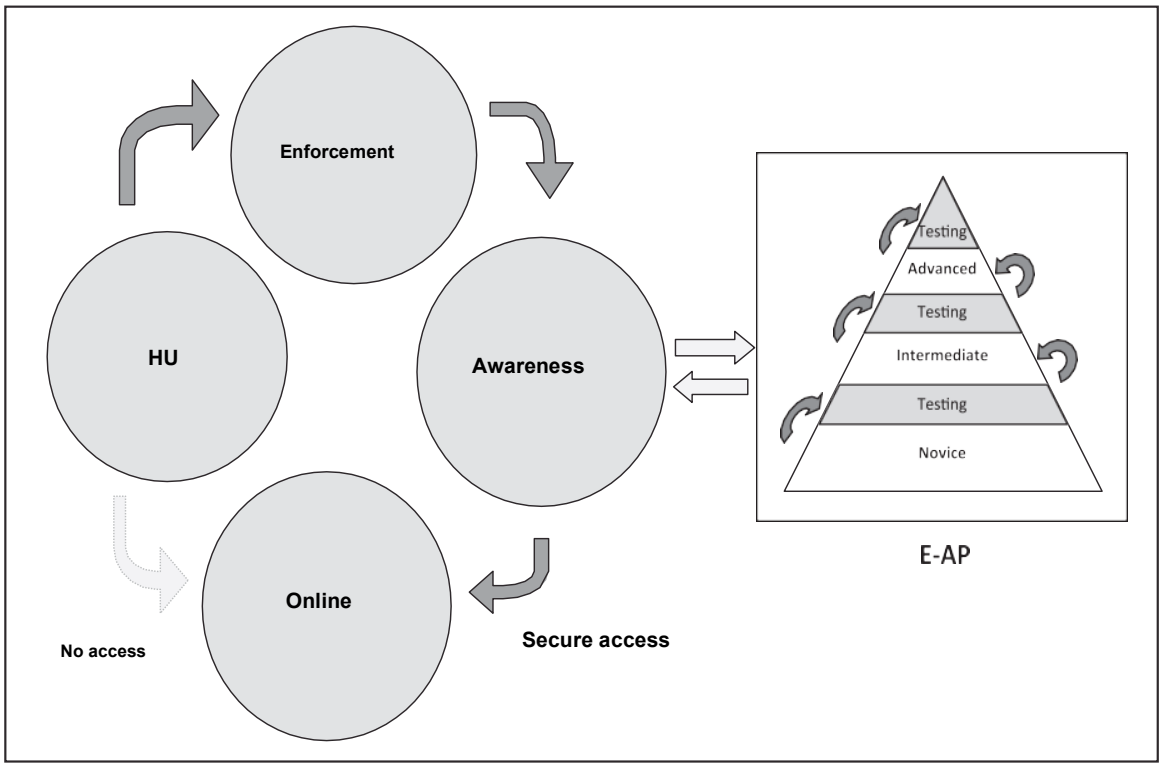

Figure 9.1: Compulsory secured access to the web for Internet users (Kritzinger and von Solms, 2010)

The most common awareness programmes are web based and are, in most cases, not easy to find and, with the level of illiteracy amongst Nigerian HUs, they may not have the skills and knowledge to find these programmes. If these programmes are found, they are, in most cases, not comprehensive enough, and do not include all relevant security issues (Kritzinger and von Solms, 2010). Furthermore, a security illiterate person will not feel the need to search for these awareness programmes online; particularly as personal information security may not be an overly important issue for Nigerians (Milberg *et al.,* 1995). In order for the awareness programme to be applicable and effective, it should be able to perform the following functions:

- Since available awareness programmes are usually difficult to find, and low importance is given to Internet security in Nigeria, the awareness programme should expose users to awareness tools to prepare them for the possible risks when accessing the web.
- There should be a check to determine if users Internet security knowledge has improved since using the programme, thereby quantifying its effectiveness.

Section 9.3 describes the development process of an awareness programme using the National Institute of Standards and Technology (NIST) framework and how it was applied in developing an awareness programme for Nigeria.

9.3 Developing the Awareness programme

The National Institute of Standards and Technology (NIST) developed a framework that aims to guide the development of an Information Technology (IT) security programme (Wilson and Hash, 2003a). For this research, the NIST framework was adapted to provide steps for developing the awareness programme for Nigeria. There are three major steps in the development of a security awareness and training programme: designing the programme, developing the awareness training material, and implementing the programme. This section describes these steps in detail.

9.3.1 Designing the Awareness Programme

The most successful programmes are those that users feel are relevant to the subject matter and issues presented (Wilson and Hash, 2003b). To design an awareness programme, it is important to understand the current security issues that will help shape the strategy and design of the security awareness programme. This involves identifying the threats particular

to Nigeria by examining the literature on current Internet security issues in Nigeria and observing and identifying the threats found in practice. This also involves investigating the most effective techniques through which the awareness programme can be delivered in Nigeria.

In this research, studies have been conducted in order to determine the awareness and training needs of Nigerian home users. The techniques used to carry out the research were:

- Interviews and surveys with Nigerian Internet users
- A review and assessment of available and current awareness topics and resources, particularly the ones more prevalent in Nigeria
- Standardised cyber-security topics that are recommended by applicable standards such as COBIT (Control Objectives for Information and Related Technologies)(ITGI, 2007)

Section 9.3.2 describes the development of the awareness material, which was determined by the results from the design stage.

9.3.2 Developing Awareness Material

The issues to consider when developing awareness material are the selection of the awareness topics. The purpose of an awareness programme is to act as an awareness raising method to focus attention on security in a way that will allow the general population to recognise security concerns and respond accordingly (Wilson and Hash, 2003b).

In determining the content areas that the awareness programme should contain, several sources were examined and analysed in order to identify the most important topics that will help raise the level of awareness. It is important to consider threats particular to the current cyber-security situation to increase relevance and effectiveness, and also consider general

cyber-security concepts in order to change behaviour and cultivate the appropriate Internet-security culture. The topics were determined from:

1. The results from the survey to determine Nigerians perception of privacy and Internet security (see Chapter 5)
2. Literature on current cyber-security issues particular to Nigeria,
3. General standardised cyber-security topics.

9.3.2.1 Nigerians Perception of Privacy and Internet Security

A study was carried out to determine the public's understanding and knowledge of data protection and privacy in Nigeria (see Chapter 5). 220 Nigerian Internet users completed a survey. The results show that there are concerns about Internet privacy and security, but the awareness about how to prevent issues is relatively lacking. This implies that although the survey participants show concern for security of their personal information, there is a lack of security awareness and knowledge. The awareness programme should, therefore, include topics that cover common self-protection techniques that will protect Internet users from cyber threats, ultimately improving their perception on Internet security.

9.3.2.2 Current Cybercrime issues in Nigeria

Although cybercrime is a worldwide problem that is costing countries billions of dollars, there are some cybercrime problems unique to Nigeria and the programme will address these issues (Hassan, Funmi et al. 2012; Longe, Mbarika et al. 2010). For instance, it is generally believed that most fraudulent emails and phishing attacks originate from or are traceable to Nigeria or Nigerians in other nations (Cukier, Nesselroth et al. 2007; Longe, Mbarika et al. 2010), therefore it would be appropriate for the programme to cover topics on these particular

issues. There are many variations of these cyber-attacks (Ibikunle, Eweniyi 2013). Some common ones are:

- Beneficiary of a Will Scam: The criminal sends e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.
- Online Charity: Fraudulent people host websites of fake charity organisations soliciting monetary donations and materials to these organisations that do not exist.
- Lottery Scam: This scam allows users to believe that they are beneficiaries of an online lottery that is in fact a scam.

Some cybercrime techniques tend to be trending at certain times, usually due to a popular event. For instance, in 2014, the Nigerian central bank introduced BVN (Bank Verification Number), which aimed at ensuring a unique identity for all bank customers. This involved bank customers filling a form, providing sensitive information. Cybercriminals used this opportunity by sending fake emails to bank customers alerting them to the deactivation or suspension of their account due to an incomplete BVN process (Muhammad, 2015). The programme should cover topics on these cybercrimes particularly ones that are currently trending.

9.3.2.3 Standardised cyber-security topics.

According to the COBIT Security Baseline (ITGI, 2007) Internet home users can be exposed to security risks mainly due to:

- Being unaware of the dangers of using the Internet
- Installing faulty or unreliable software with security weaknesses
- Using out-of-date operating systems, security software and application software

- Being exposed to information and identity theft through viruses, spyware, spam, phishing and other attacks

The ENISA (2010) report suggests that topics like e-mail, electronic communication, passwords and security updates are very important not only to businesses but also to home users. Based on their conducted survey, it was concluded that the following security areas are important for Internet users.

- Security policies and procedures.
- E-mail security.
- Social engineering.
- Identity verification.
- Technical security mechanisms.
- Phishing
- Incident response

After developing the awareness material, the next stage of the process is implementation. This involves identifying appropriate delivery methods and relevant stakeholders that could implement the programme. These are discussed in Section 9.3.3.

9.3.3 Implementing the Awareness programme

To implement the awareness programme, a selection should be made of the methods through which the messages will be delivered and the organisations that will implement the programme.

9.3.3.1 Training methods

The different means of transferring security knowledge are through formal training sessions, strategic placement of awareness messages, web-based training, interactive computer-based training and contextual training (Chapter 2, Section 2.5.3). However, as initially discussed (see Section 9.1.2), using these methods alone may not be effective enough in improving Internet-security culture in Nigeria. This study suggests implementing both contextual and web-based training as a combined method. This ensures that both information and knowledge are context specific and in relation and relevant to the cyber-risk associated with the current action being undertaken.

Kritzinger and von Solms (2010) suggest an enforced awareness where each level will have a testing environment where the HU can be evaluated regarding the material for each level before moving to the next level (see figure 9.1). However, this compulsory process might be cumbersome as it forces Internet users to complete the programme before making use of the Internet. The study described in this thesis suggests that Internet users should gain awareness when making use of the Internet rather than before (Chapter 8, Section 8.2.2). Figure 9.2 shows a description of this process. The Internet user would be encouraged to gain awareness at certain times, such as when visiting a potentially dangerous website. Internet users will be redirected to a warning page providing a brief description of the threat and then they will be requested to go through a brief awareness programme with the relevant content.

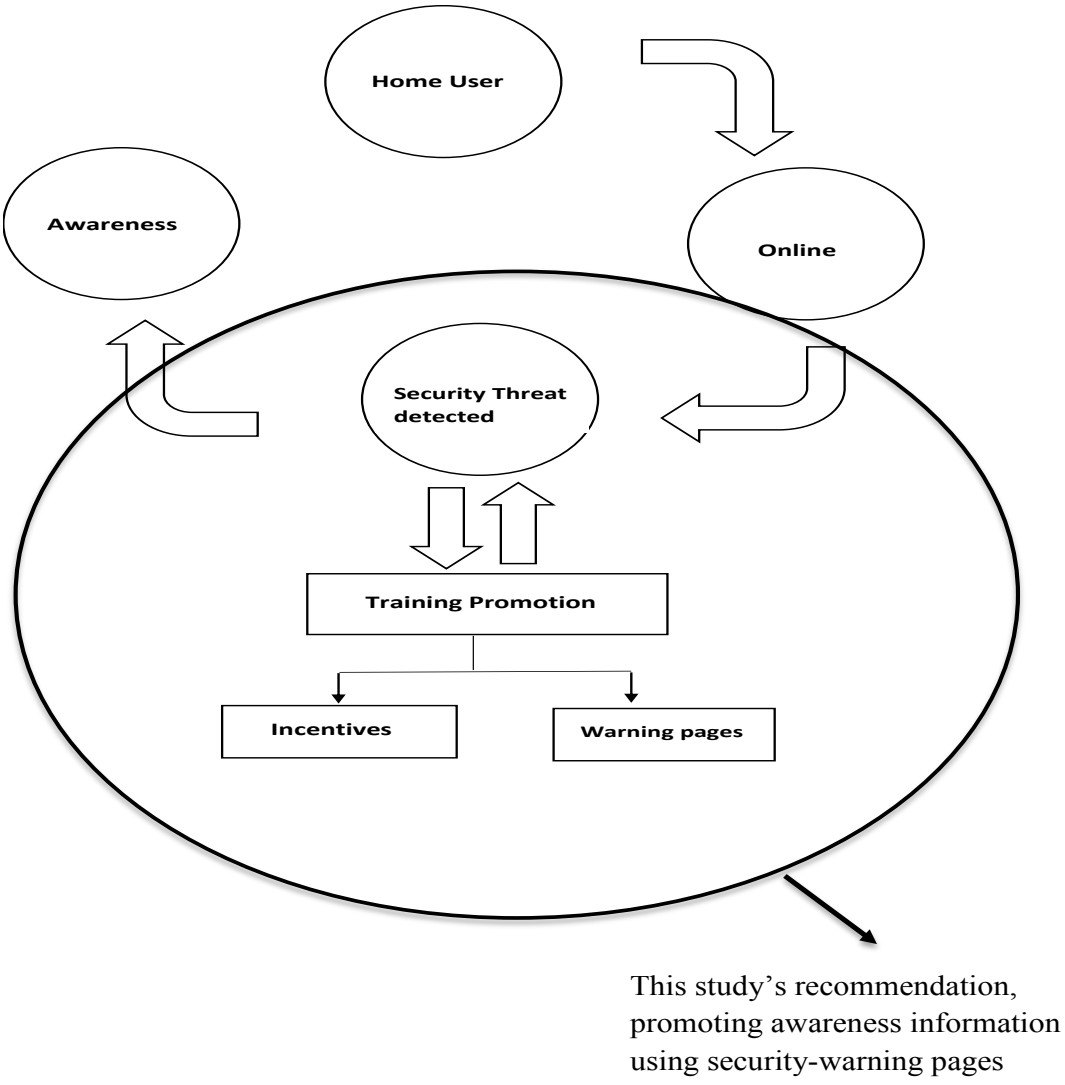

Figure 9.2: Awareness training

9.3.3.2 Awareness programme stakeholders

Another important aspect is to determine which organisation will implement the programme. Some organisations that could potentially implement the programme are:

- **Governments** usually organise cyber-security awareness programmes for the citizens to encourage good online practices. These usually involve online resources in the

form of resource websites and campaigns in the form of posters and advertisements. Nigeria currently has ngCert (Nigerian Computer Emergency Response Team), which was created as a result of the new Nigerian cybercrime bill (ngCert, 2014) (see Section 9.1.2.1).

It was found that the Nigerian government may not be able to implement the proposed awareness programme due to some identified factors, for example socio-economic priorities and reputation (see Chapter 7, Section 7.1.1). However, this study recommends that the government should be involved in research, which includes awareness-raising methods and collaborate with private organisations (see Chapter 8, Section 8.2.1). For instance, they could provide incentives for private institutions to provide awareness programmes for their customers.

- **Internet service providers (ISP)** provide some awareness for their customers on Internet security issues and how they can manage them. They assist customers to protect themselves from online threats, for example by anti-virus and anti-spam software (HM Government, 2013). In the case of Nigeria, telecommunication companies are also major Internet service providers. The proposed type of awareness programme could be implemented by the ISPs to educate their customers before they use their services.

  They could integrate the awareness programme to their security warning pages to enable users to have the opportunity to know more about the threats when the page displays.

  This could potentially protect their customers from dangers online and, at the same time, enable them to provide better services and reduce strain on their services due to

unwanted traffic such as spam mail and distributed denial-of-service attacks on their network.

- **Academic institutions** educate young people to use the Internet securely and safely. This is usually in the form of outreach and awareness programmes organised by internal and external security professionals (McCoy and Fowler, 2004). Another common method is integrating the Internet security resources into school curriculum to equip students with practical cyber safety skills and knowledge (McGettrick *et al.,* 2014). Academic institutions could implement the proposed awareness programme by integrating it to their network, especially on public computers. This allows the users to have access to awareness material when on the institutions network. This will allow awareness training to not be limited to in-class or formal training sessions.

- **Financial institutions** provide awareness for their customers on Internet banking security issues on their website, emails and newsletters. However, a financial institution (for example a bank) could integrate the awareness programme into their online banking platform to give customers access to awareness material relevant to ensuring their financial information is safe.

  This could potentially reduce identity theft and fraud complaints and at the same time improve their overall services to their customers.

Based on the findings of this research (see Chapter 7), it is recommended that private institutions should implement and monitor the awareness programme. This programme would be more effective if regulated by a non-government organisation who would benefit from their customers' improved awareness and Internet-security culture. Even though an organisation uses the best technical solution to provide adequate security, without the perception and awareness from customers these solutions may not be useful.

The institutions with the potential to provide and manage awareness programme are Internet service providers (ISP), telecommunication institutions and financial institutions that have prominent roles in the use of the Internet and e-commerce in Nigeria. These institutions could design the awareness programme based on the services provided and on their customers' needs. For instance, an awareness programme developed by a financial institution would focus on financial related cyber threats.

These organisations could encourage Internet users to go through the awareness programme through incentives such as free data storage for customers who visit the programme to improve their security awareness. An effective government could also regulate the programme. However, in the case of Nigeria, the government may not be currently effective enough to solely regulate this programme because of their known ineffectiveness and the other priorities a developing nation would have (Central Intelligence Agency, 2015). The programme described should make sure Nigerians are regularly exposed to Internet security content, which, in turn, will improve their views on the importance of personal information protection, increase Internet literacy and create a general Internet-secure culture in Nigeria.

9.4 Conclusions

Accessing the web has many risks for the home users who have limited Internet security knowledge. It is, therefore, essential to ensure that users are educated and understand the risks involved and how to limit them. In the case of Nigeria where there is a significant lack of awareness and absence of regulatory body, an awareness programme should empower users by giving them a better understanding of security issues, possible threats and how to avoid them. However, it is not enough to just provide an awareness programme, it is also important for citizens to easily find and make use of these awareness resources. This study

suggests that making use of an enforced awareness programme will not only provide an Internet security awareness programme, but also ensure it is being used effectively. However, the form of enforcement described does not force the Internet users to gain awareness by being a compulsory prerequisite before using the Internet. It ‘enforces’ awareness by ensuring Internet users gain awareness when using the Internet via warning pages and incentives, making it more of a promotion of awarness. It is also suggested that private organisations that are involved in e-commerce should implement and monitor the programme. Promoting a good Internet security culture will make online customers aware of websites, which make use of good security procedures and policies and those that do not.

The next chapter focuses on the implementation and evaluation of the prototype to assess its effectiveness and applicability of the recommended training method. Surveys and focus group discussions were conducted with potential users and providers to get their opinions, suggestions and validation of the programme.

Chapter 10: Development and Evaluation of the Awareness Training Method

Chapter 8 discussed Nigerian Internet home-users and the lack of Internet security awareness and suggested there is always a need for promoting Internet security awareness. It also described the awareness programme in detail and proposes methods for developing and implementing the programme. A prototype of the awareness programme was developed in order to provide insight into the effectiveness of promoting the awareness programme in which users are given warnings and an opportunity to undertake training based on the activity they are conducting, but are not forced to take the training.

Having recommended an awareness programme, there is a need to test its validity before it can be more widely disseminated. The aim of the validation process is to determine whether the research recommendations are effective and, also, to establish whether they are reliable. Section 10.1 provides a general discussion of the development of the prototype then the method adopted for undertaking the validation exercise. Subsequently, the details involved in each of the validation procedures and the results are discussed.

10.1 Development of the Awareness Programme

This section will examine the implementation and evaluation of the programme, particularly the process of putting the prototype into action and aspects of the development work behind it. To evaluate the awareness programme based on security warnings and contextual training, the topics are presented in a brief and simple manner with more focus placed on the manner in which the awareness programme will be accessed when online.

Chapter 9 suggests possible topics that could be included into the awareness programme based on Nigerians perception of privacy and Internet security, literature on current cyber-

security issues particular to Nigeria and general standardised cyber-security topics. However, when developing the prototype, for proof of concept, only two topics where included in the programme:

- Social Engineering
- Internet and Email security

Social engineering involves a combination of techniques used to manipulate victims into divulging confidential information; such techniques include impersonation, phishing, advance fee fraud and their variations (Atkins, Huang 2013, Bullée, Montoya et al. 2015). These attacks are not technical in nature and involve communication technologies with which the users are engaged on a daily basis. This is a very common technique used by fraudsters in Nigeria thus it is important that users are familiar with its different variations so they can be prepared.

The Internet and email security topic describes how Internet services such as e-commerce work along with the risks associated with them. It also describes how attackers can distribute malicious code and the defences against such attacks along with security risks associated with the use of e-mail and methods of protection.

10.1.1 Prototype Development

10.1.1.1 Content Layout

In designing the user interface, interactive strategies were applied in an effort to engage the users (CDC, 2013). The prototype was developed having in mind the requirement for ease of use by the user plus efficiency in navigation and material coverage. The interface, in order to be learner-friendly, should include a main menu and the necessary navigational elements that help the users know where they are within the course and how they can easily move through

it. The main purpose for developing the prototype is for proof of concept (i.e. promoting awareness with contextual traing). The following functions were applied when designing the interface and the navigation elements of the awareness programme:

- The navigation is clear and easy to use
- The next and previous buttons are easily located.
- The content can be easily found by users

The content is indexed so that learners can find the information they seek easily. Taking these best practices into consideration, the prototype screen consists of the following areas:

- **Menu area (1):** The menu area displays the different areas of the programme. The title of each area works as a hyperlink and the user can jump directly to any part of the programme. The resources tab contains useful links and documents on the topic area of security awareness
- **Main window (2):** The main window displays the actual contents. These include the content menu, which consists of the title of each area and works as a hyperlink so that the user can jump directly to any part of the programme. See Figure 10.1.

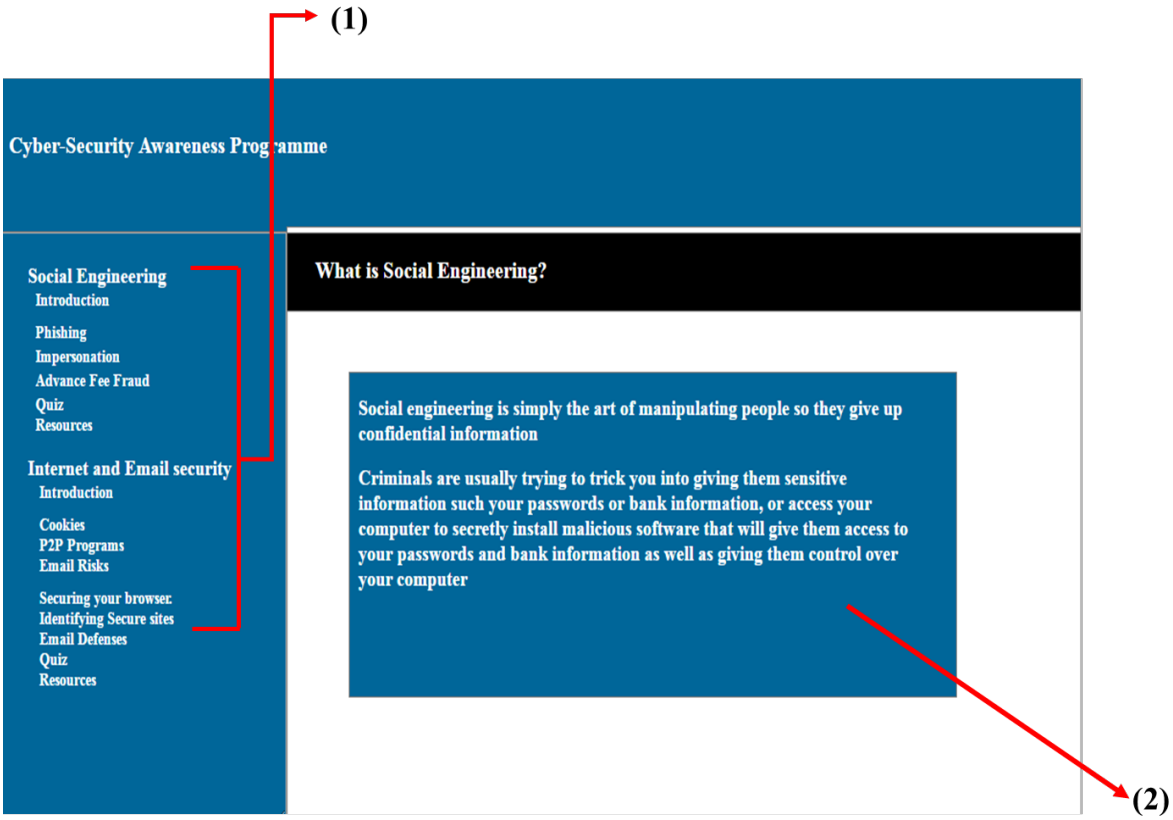

Figure 10.1: Prototype of the main window

10.1.1.2 Programme Content

The programme starts with an introductory screen, which contains the table of contents. Each topic has a content area and a quiz area.

The topic that deals with social engineering focuses around the following areas:

- **Introduction**: Social engineering is defined as a way cybercriminals manipulate Internet users into divulging confidential information.
- **Phishing**: This section explains what phishing is and how hackers attempt to acquire Internet users' sensitive information by setting up a replica of an original website

(Ramzan 2010). Common techniques used to deceive the users and how to recognise a fake website are explained.

- **Impersonation**: This section describes what impersonation techniques hackers use and how to prevent impersonation.

- **Advance fee fraud (419 Scams):** Advance fee fraud is described in the programme as tricking prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return for providing some modest payment in advance (Smith, Holmes et al. 1999). This type of scam originated from Nigeria and is primarily carried out by Nigerians and is commonly referred to as 419 scams (Oriola 2005).

The topic that deals with Internet and email security focuses on the following areas:

- **Introduction**: This section describes how Internet and related services work along with the risks associated with them.

- **Cookies**: This section describes what a cookie is, how cookies work, how hackers could steal cookies and how to enable/disable cookies.

- **Email risks and defences**: This section provides tips on how to spot spam and phishing emails, the risks from such emails and tips on how to use email safely.

- **P2P Programs**: This section covers what Peer to Peer programs (P2P programs) are and the dangers of using them to share files such as viruses, spyware, adware and identity theft.

- **Securing your browser**: Popular web browsers such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari are used frequently, therefore it is important to

configure them securely. This section discusses the problems an unsecured website could bring and gives tips on how to secure a web browser.

- **Identifying secure sites**: Although e-commerce has its advantages, the risks are there. In addition to websites with questionable business practices, some websites are used by scammers, posing as retailers, in order to steal unsuspecting customers' credit card or other personal information. The awareness programme provides information on signs to tell if a website is genuine and things to look for in a secure website.

The Sections 9.2 and 9.3 describe the evaluation process and the results.

10.2 Validating the Effectiveness of Promoting Internet Security Awareness through Contextual Training

An awareness programme is considered effective if it is capable of establishing the appropriate knowledge and influences the attitude and behavior of the participants towards positive changes in their security culture. The validation of a model/framework is the process of confirming whether the proposed model/framework is appropriate, especially in the light of the purposes of the investigation (Frees, 1996).

In order to provide insight on the effectiveness of the awareness programme, quantitative data needs to be combined with qualitative data to determine if the desired effects have been achieved in terms of user behaviours (Veseli, 2011). The methods adopted are surveys and focus groups.

10.2.1 Selection of the Participants for Validation

Three options were considered for carrying out the validation: (i) focus groups ,(ii) interviews and (iii) surveys. The use of interviews was not selected due to time, cost and location constraints, leaving the survey and focus group as the most appropriate options.

Problems associated with surveys such as the restrictive nature of the questionnaire and lack of opportunity for respondents to clarify their answers were overcome by carefully designing the questionnaire and making some questions open ended. It is important to validate the suggested programme with Internet users and experts such as employees from relevant companies such as those involved in e-commerce, banking and telecommunications.

A covering letter was sent to the 15 experts, however, just 11 responded to the requests. The expert participants were chosen from relevant organisations including participants that were initially selected for the purpose of validating the recommendations (see Chapter 8) requesting their kind assistance in the validation exercise and restating the purpose of the research. The experts were referrals and recommendations from the researcher's professional contacts. The questionnaire was attached to the prototype highlighting what is expected of them for the validation process (see appendix C). This was sent out via email to the participants and reminders were also made over the phone and email.

The Internet user participants were selected randomly but according to the specific criterion of Nigerian Internet users. The main purpose of the awareness training programme is to improve the digital illiteracy amongst Nigerian Internet users, hence the criterion. In total 136 participants were involved in the study. A link to the survey material (Qualtrics) was distributed via the researcher's social networks (Facebook, Twitter and Blackberry Messenger) and email. The researcher also enlisted the help of her colleagues by requesting that they post the links on their social networks to get more participants.

Apart from the survey method, the researcher also conducted a focus group. An introductory email was sent to the seven selected participants who participated in the questionnaire, requesting their assistance and participation in the focus group and highlighting the importance of study. The researcher initially narrowed down the participants based on their age (between the age of 18-40) and how frequently they used the Internet, this was determined by their answers in the initial questionnaire. Afterwards they were further narrowed down based on their availability and willingness to be available at a specified location to conduct the focus group at a day and time specified by the researcher. The focus group was conducted via video chat (Skype) due to the required participants being in Nigeria and the researcher being in the United Kingdom.

The rationale for choosing this group is to investigate how young Internet users would perceive using the security awareness programme. Previous studies have found the majority of those who regularly use the Internet are within this age group (Broadcasting Board of Governors, 2014). Furthermore, some of these young people will become key decision-makers in information technology (IT), and this age group, as a whole, will need to confront privacy-related issues to a degree that older people will not. Therefore, it is important to get their opinion on the awareness training programme (Miltgen and Smith, 2015).

Section 10.2.2 describes the validation process followed by conclusions drawn from the findings.

10.2.2 Methods for Validation

As stated in Section 10.2.1, two methods were adopted for the validation exercise, which were a survey and a focus group. In order to verify the effectiveness of promoting internet security awareness through contextual training, the developed prototype was sent to all the participants to get their opinions and experiences of using it.

10.2.2.1 Focus Group

The focus group was used to assess the effectiveness and usability of the proposed awareness programme.

The focus group participants were asked to go through the prototype website similar to that used for the survey. The focus group involved conducting an open discussion concerning the experience of the participants in using the programme, a series of questions (see appendix C) was prepared for this purpose.

The focus group was scheduled to last no more than one hour. The online programme participant experience was recorded using screen capture software and the discussions using a voice recorder. The participants were informed of the recordings in each case. In order to prevent the recordings from affecting their behaviour, the participants were given information about what was being studied, this being limited to seeing how they would react to website conditions so there would be no recording of their views or opinions. None of the participants objected to their actions being recorded in these circumstances. The participants were then asked to navigate a prototype e-commerce website and act as they would normally when navigating a website.

During the exercise, a pop up message notified the participant of a threat on the website and provided a brief explanation of the threat. The participants were then invited to go through cyber-security training on the issue. The aim of this exercise is to verify if promoting cyber-security awareness through this method will be effective. This was ascertained by determining if the threat prompt was enough to compel the participants to visit and go through the awareness programme.

10.2.2.2 Survey (Internet users)

When the participants used the prototype website, they were redirected to a warning page providing a brief description of the threat and a request for them to go through a brief awareness programme, though they had the option to ignore the issue. After the exercise, the participants were asked to fill a brief questionnaire. 136 participants completed the questionnaire. The questionnaire began with a set of demographic questions about sex, age and education. This is summarised in table 10.1

Table 10.1: Survey participants (Internet users)

	N=136
	Percentage
Sex	
Male	47%
Female	53%
Age	
18-20	14%
21-29	41%
30-39	25%
40-49	15%
<50	5%
Education Qualifications Completed	
PhD	4%
Master's Degree	34%
Bachelor's Degree	41%
Undergraduate	17%
School Certification	2%
Primary School	0%
Others	2%
Occupation	
Student	23%
Job in private sector	37%
Job in Public sector	12%
Unemployed	8%
Self employed	20%

10.2.2.3 Survey (Experts)

The programme's effectiveness was tested using a group of individuals that are considered experts in their field. The participants are involved in IT and e-commerce such as IT and cyber-security consultants in various organisations. This testing was done by exposing the group of experts to the prototype website similar to that used by the Internet users, and their opinions were measured and analysed through an open-ended survey. In terms of job function, the participants are classified in table 10.2.

Table 10.2: Survey participants (experts)

Job Function	**Participants**
IT department (banks)	3
IT Administrators (Telecoms)	3
IT department E-commerce firm	3
Government officials	2

The experts that participated are considered qualified individuals academically because of the nature of their employment with experience in their field of expertise and, therefore, their opinion is considered valid and credible.

- The three bank employees comprised of two security analysts and one IT auditor and are working for big banking industries. The security analyst job responsibilities include assisting with security threat detection, prevention and management. The IT auditor assists in creating and maintaining policies and procedures regarding network security.

- The IT administrators are members of the IT departments in telecommunication companies, which provide Internet services. Part of their job description is detecting and managing Internal and external security threats.

- The IT E-commerce firm employees are part of the customer service team and deal with everyday security related user problems.

- The government officials work in top management positions. Although they are not directly in IT positions they are actively involved in Internet security

Representative Screenshots of the Prototype Website

Figure 10.2 shows an introductory page highlighting the background of the study and what was expected of the participants.

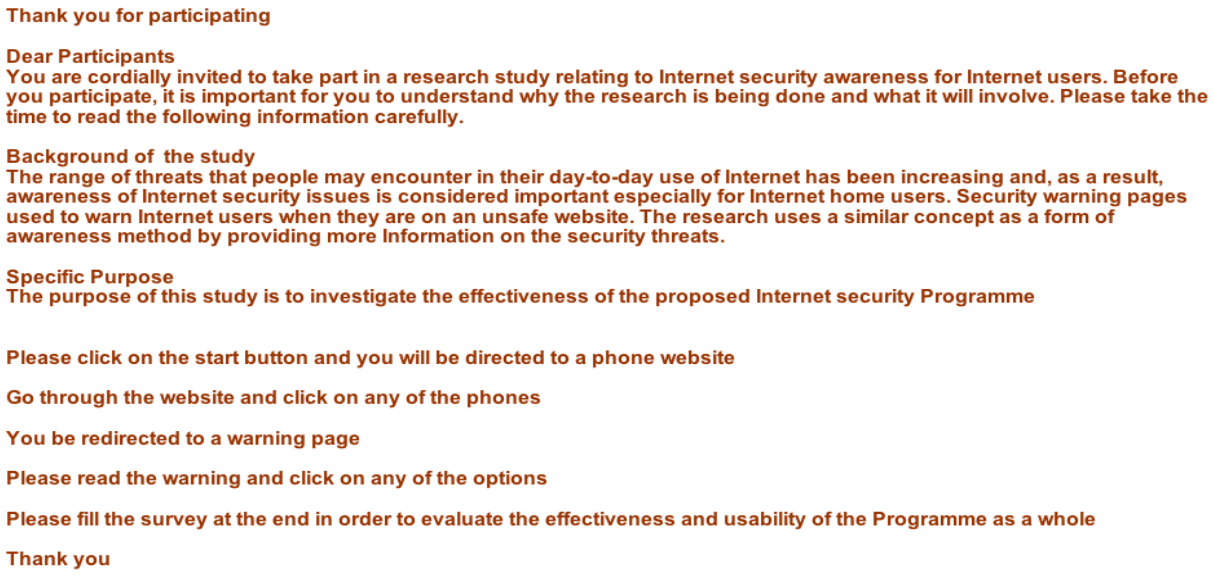

Figure 10.2: Introductory page

Figure 10.3 shows the prototype website's homepage. Participants were asked to navigate the website as they would usually do.

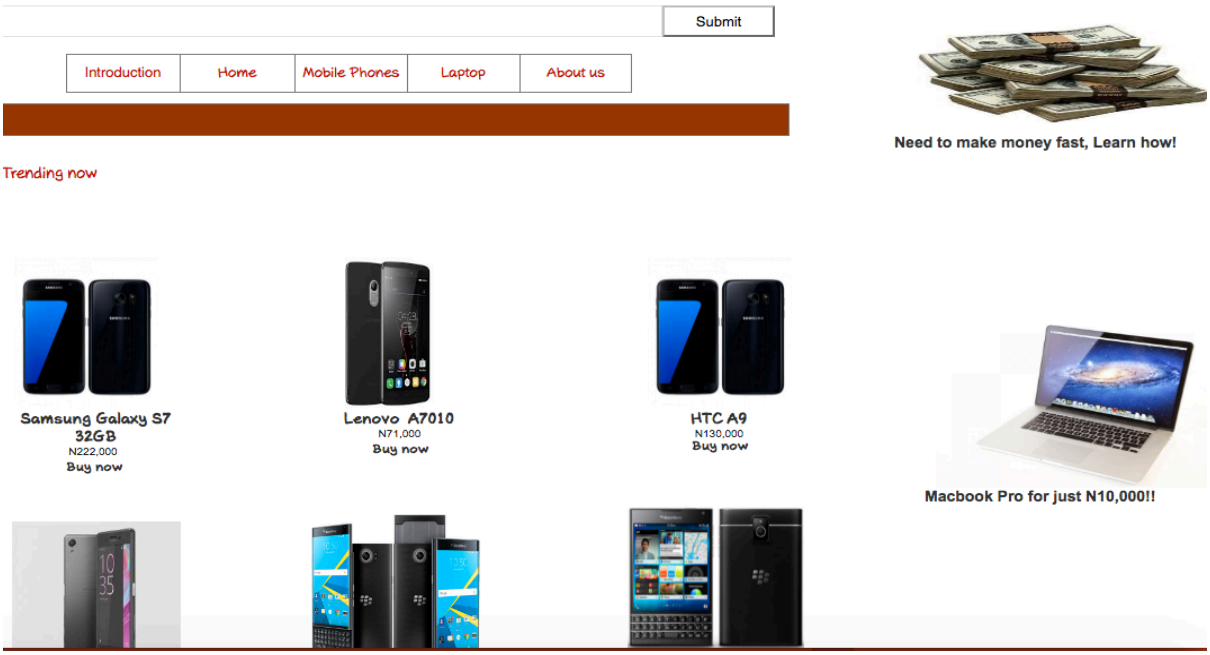

Figure 10.3: Prototype website home page

When navigating the website, the participants were redirected to a cyber threat-warning page.

Figure 10.4 shows the security page

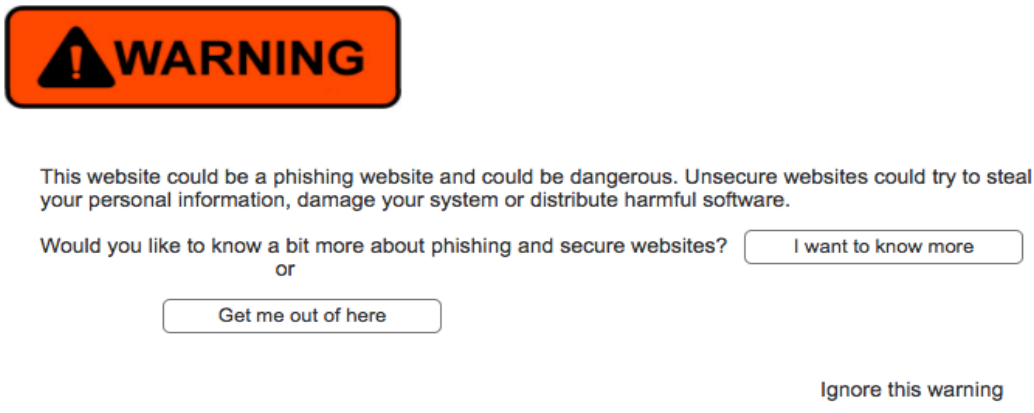

Figure 10.4: Security warning page

If participants choose to know more about the threat, they were redirected to the relevant content based on the context of the security alert. This is shown in figure 10.5.

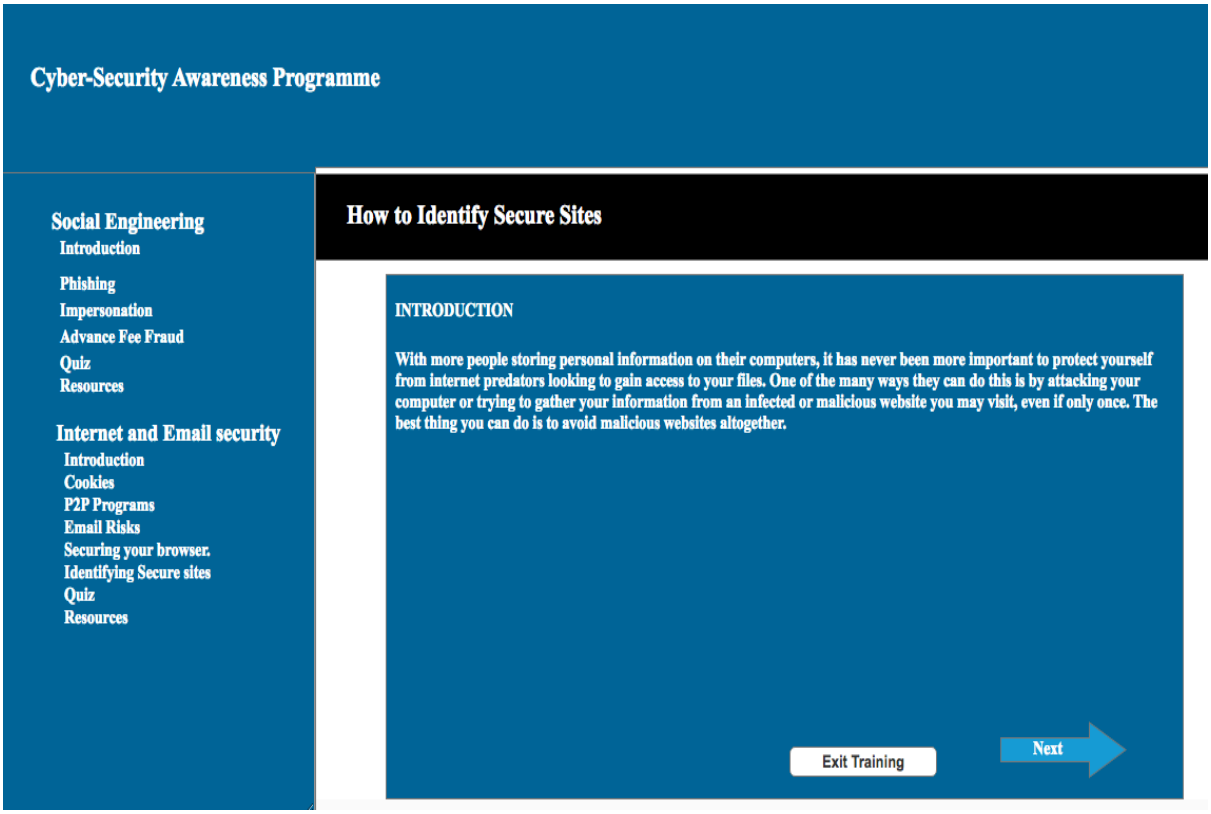

Figure 10.5: Participants opt to know more

The results of the validation are discussed in Section 10.2.3.

10.2.3 Participant's response

This section describes the results from the validation discussed in Section 10.2.

10.2.3.1 Focus group results

The study involved a group of seven Nigerian Internet users who make use of the Internet daily.

Six out of the participants had not been exposed to any Internet security awareness programme, one did courses on security issues during their undergraduate studies. The participants showed interest in the security awareness programme and the way it was

delivered, especially in the case where it could be used as a substitute to a traditional security warning pages which either warns users of a threat without providing more information on the threat, or even blocks the users from using the website. Although the participants generally accepted that the tool would work as a substitute for the usual awareness programmes, especially since these programmes are not readily available for Internet users, some of the participants agreed that they would usually ignore the prompts. Two of the participants indicated that they would not ignore the warning and would proceed to find out more on the issue as they are usually concerned for their safety when online. All of the participants agreed that that including incentives in the programme would increase interest in the awareness method making its purpose more effective.

One of the participants suggested that the banks should implement a similar approach, especially in their Internet and mobile business, as financial cybercrime is very common and most of the phishing scams are bank related. It was also suggested that the awareness training itself, when implemented, should be very brief and contain fewer words.

10.2.3.2 Survey Results (Internet Users)

The study was focused on Internet home users all the participants make use of the Internet daily. After viewing the website, the participants were asked if they read the security threat prompt. Nearly all (95%) of them read the threat alert Although many of the participants paid attention to the security prompt, more than half of them (58%) chose to ignore the invitation to opt for the awareness programme.

Table 10.3: Why didn't you visit the link?

Answer	%
Did not understand the prompt	15.2%
Uninterested	24.2%
Already know about the issue	10.6%
Could easily visit another website	40.9%
Others, please specify	9.1%
Total	100%

Half of the participants agreed that the method is an effective way of improving Internet security awareness. 42% of the respondents followed the awareness link on the webpage with 37% of them going through most of the programme.

Table 10.4: How much of the programme did you go through?

Answer	%
All of it	28.6%
Most of it	36.7%
Just a little bit	26.5%
Left after the first page	8.2%
Total	100%

On a positive note, 74% of the participants stated that they would go through the awareness programme if there were an incentive, with 43% of the participants preferring internet data as an incentive. Furthermore, 71% of those who did not visit the link indicated that they would do so with an incentive.

Identifying relationships between variables was an objective of the analysis of the questionnaire results to gain a better understanding of the outcome. The chi-squared test ($\chi 2$) is used to test hypotheses. The test was applied to show the relationships between the responses gathered using a null hypothesis, which states that there is no relation between the responses. An analysis was done to find out if there is a relation between the participants that thought the programme was an effective way of promoting cyber-security awareness and those that went through the programme (see Appendix C for full results). The chi-squared test shows clearly a relation between both responses ($p<0.05$). Responses show that majority (60%) of those who went through the entire programme strongly agreed that it is an effective way of promoting cyber-security awareness.

10.2.3.3 Survey Results (Experts)

Eight out of the participants agree or strongly agree that the approach would be effective in promoting cyber-security awareness for their customers. It is also important to note that both government officials noted that there are no current functioning awareness initiatives.

Both government officials stated that the programme was easy to understand and would be effective in promoting Internet security awareness. One of the e-commerce firm employees stated that, although the programme will be useful in promoting Internet-security awareness, constant security prompts may make e-commerce users feel more threatened and, in turn, this may prevent e-commerce growth. An IT manager at an e-commerce firm stated that their company makes use of hardware and software firewalls to protect their customers' data, however, there is not any current awareness programme being implemented for their customers. They were positive about the applicability of the programme, and said "I believe this programme will help individuals identify and learn to avoid or deal with cyber threats".

One of the bank employees stated that it would be useful to integrate user tests into the awareness programme, which would alert the users of gaps in their knowledge when going through the programme, in order to ensure that the awareness course is successfully completed. Another bank employee stated the approach would be useful in promoting awareness to their customers which would, in turn, improve their services too if customers are aware of cyber threats and prevent them before they occur.

One of the telecoms employees agreed that the approach could be beneficial for their company in terms of reducing cyber-security problems, considering that there is not any current initiative being implemented. However, he stated that the cyber-security awareness programme could be more effective if it were more visually pleasing for customers. Another telecoms employee stated that they implement ISMS (Information Security Management System) awareness courses for their employees.

10.3 Implications

The primary finding is that promoting Internet awareness through security warning pages can be very effective in practice, especially if implemented with appropriate incentives.

10.3.1 Security Warning Page

Popular opinion holds that browser security warnings are ineffective (Akhawe, Felt 2013). However, the study demonstrates that browser security warnings can be effective at prompting users to know more about the security threats. Although more than half the participants chose to ignore the warning and not proceed, a relatively good number (42%) chose to know more about the security issue and more than a third (37%) completed most of the programme. If this was provided for the whole population of Nigerian Internet users, and

if it had a similar success rate, then this would be a very significant step forward and would greatly reduce the awareness gap in the population.

10.3.2 Internet security awareness through Incentives

Furthermore, the survey responses indicated that this success rate would greatly increase to three quarters of the population if a suitable incentive could be given. This would represent a very significant step to removing the awareness problem altogether. This approach could revolutionise how Internet users access and view Internet security awareness. Security warning pages could become a way of alerting users to cyber threats and simultaneously be a method of distributing awareness programmes. Internet users would be able to identify cyber threats, understand the consequences of the threat and know how to avoid the threat when using the Internet.

Studies have shown that when an incentive is offered for an action, attitude and recognition towards a course can be improved (Lohtia, Donthu & Hershberger 2003). This is further supported by the survey results. However, it is important to note that since the training programme is in the form of contextual training, a small incentive may be enough to persuade Internet users to go through the awareness programme. Ideally, organisations that implement the programme would need to provide incentives relevant to the services they provide, such as additional Internet storage space being provided by an Internet Service Provider. An example from a bank could be improved insurance or reduced bank charges for certain activities or even an extended overdraft facility.

10.4 Conclusion

The study seeks to understand how Nigerian Internet users perceive a continual Internet security awareness programme when online. With the current lack of privacy laws and poor privacy practices, and prominent cybercrime, this study demonstrates that exposing Internet users to awareness content via security warnings pages can be an effective method of promoting awareness security training.

The programme's validity was evaluated using a survey which participants were exposed to the awareness programme and their thoughts where collected via a questionnaire. Further to that, the programme's effectiveness was tested using a focus group where the group's thoughts were discussed and presented. Finally, the programme was tested using a group of experts by exposing them to the programme and measuring their opinions via a survey. From all testing methods, the programme was shown to be a valuable and effective means to establish a greater level of security awareness amongst the Internet users. The results indicate that the success of the programme could be further improved with the inclusion of incentives, as many of the participants stated that including incentives would motivate them to go through awareness training.

Chapter 11 Conclusion

This is the final chapter in this thesis. It begins by providing a summary of the major research findings. It presents the research contributions and implications, achievements and limitations and, finally, a summary of findings and suggestions for future work.

11.1 Achievement of the Research Aim and Research Objectives

The main aim of the research (see Chapter 1, Section 1.5), which is to identify and develop strategies that will enhance e-commerce privacy and data protection in developing nations, has been achieved having identified strategies, which have led to the development of a framework that can assist in resolving problems facing privacy and data protection in Nigeria. This should improve trust issues regarding performing transactions online and inevitably improve e-commerce adoption in developing nations. Although, from the analyses of literature, an overall understanding of Internet privacy and data protection was gained, the majority of existing research is based on western countries and their experiences as fewer researchers have focused on developing countries.

The first research objective considered previous and related work done in the research area to see what has already been done to identify the e-commerce data protection and privacy problems in developing countries, and in Nigeria in particular, and to identify what approaches have been adopted in developed countries and in Nigeria (see Chapter 2). The research was able to identify two major approaches being adopted in different countries; these are government regulation and self-regulation. The research used the United Kingdom's data protection act as a government regulation case study. The UK Government implemented an EU Directive in the form of the Data Protection Act in 1998. The act includes principles which provide guidelines and specifications for collecting and processing

personal data and all e-commerce websites are required to have a privacy policy that informs the website's visitors how data can be retained, processed, disclosed and removed in line with the principles. In the self-regulation approach, data protection in an e-commerce context is left mostly to the evolution of industry norms and voluntary compliance. The research used the United States as a case study of the self-regulation approach. Each company is responsible for deciding on the degree of information that is collected and used, and for developing its own privacy policy statement based on its industry guidelines.

In the Nigerian context, the constitution recognises the right of privacy, however, Nigeria has not yet legislated any specific data protection law comparable to that in operation in other countries like those in the European Union, nor dos it have an effective self-regulation system like that in the Unites States. The closest that Nigeria has to a data protection legislation is the Draft Guidelines on Data Protection published by the National Information Technology Development Agency. The draft guidelines have little legislative authority which, therefore, makes the guidelines ineffective.

Due to absence of any existing effective data protection and privacy approach, the second objective addressed the applicability and effectiveness of the current approaches used in the case study countries. This was achieved by evaluating the approaches' dispute resolution, enforcement and compliance monitoring processes for their possible applicability in Nigeria. Benchmarks developed by the Australian government for Industry-Based Customer Dispute Resolution Schemes provided a suitable mechanism for evaluation (see Chapter 7). Any approach that may work in Nigeria should have a dispute resolution system that is very easy to access and understand and will involve less government involvement and a strict compliance monitoring system. The study revealed that the self-regulatory approach is likely to be more effective in Nigeria, although some of the aspects of this approach may be

ineffective due to lack of awareness. However, if customers became more aware of the importance of data security and privacy, then public and commercial pressure would encourage organisations to take up a voluntary self-regulatory approach.

In order to determine some of the privacy and data protection issues in Nigeria, the third research objective was to confirm the existence of a problem in the e-commerce privacy and data protection approach in Nigeria. 65 websites' policy content were analysed to gather information about the websites' policy practices (see Chapter 6). The content analysis has revealed that these policies fail to provide information about important areas of privacy. It was discovered that although the majority of the websites make use of cookies and third party cookies, many fail to disclose information about this practice. Overall most of the websites fail to adequately fulfil the general guidelines for good privacy practices and significant improvements are needed in this regard. This limitation could be because of the current lack of efficient enforcement and compliance monitoring. It can be suggested that standards and principles tailored to the current e-commerce industry in Nigeria are necessary. The standard should include compliance monitoring and enforcement for e-commerce websites that would encourage good privacy and disclosure practices.

The fourth objective was to determine factors affecting privacy and data protection in developing nations, particularly Nigeria. It was determined that cultural values and privacy perceptions differ from country to country (see Chapter 7). These varying values exert a significant influence over how privacy is respected and treated in a given country. This, in turn, determines which data protection approaches a country adopts or if a country has effective data protection. The research was able to identify six Nigerian factors that affect privacy and data protection in Nigeria:

1. The first factor is a lack of effective government law enforcement, indicating that the government may not be effective enough in developing initiatives or legislative solutions for privacy and data protection.
2. The political view of a country is also a factor that can affect its view on data protection. The attitudes descending from the past totalitarian regime in Nigeria could be a factor influencing the nation's slow adoption of a data protection policy.
3. Another factor is the economic priorities as Nigeria, being a developing country, needs to focus more on other pressing economic issues, such as electricity and education, so enactment of a data protection policy would not be the government's highest priority. Due to these other problems, the nation's government may not be overly concerned about the need for data protection to protect their citizens or corporations.
4. Studies have shown that regulatory responses usually occur in reaction to a growing level of information security concern within the masses. Studies also suggest that lower levels of information privacy concern will be associated with countries with no privacy regulation.
5. The fifth factor is the high level of digital illiteracy and lack of awareness of IT risks coupled with the relatively high Internet adoption, which makes a high proportion of the Internet users vulnerable to the privacy and data protection dangers in Nigeria.
6. The final factor is the high cybercrime originating from Nigeria, which has given the country a bad reputation within and outside Nigeria. This reputation and the lack of trust it generates creates a need for data protection, but at the same time, inhibits the population from trusting any scheme that could be put in place to protect personal data.

The fifth objective was to determine the general knowledge and perception Nigerians have about e-commerce and its dangers, data protection and privacy by conducting surveys and Interviews (Chapter 5). The summary of the findings is that the majority have accepted the disclosure of personal information is necessary for e-commerce but appear to be minimally concerned about providing personal information unless financial information is concerned. The advantage of there being little concern about companies misusing their personal information is that this could lead to a rapid growth of e-commerce. However, the downside is that their lack of concern could mean that the Nigerians are vulnerable to their information being misused.

The sixth research objective identified strategies to improve general awareness of the dangers of e-commerce, privacy and data protection (see Chapter 8). Empirical data based on the results obtained during the data collection assisted in identifying strategies for improving Internet privacy and security awareness. The recommended strategies became part of the developed framework. The research established the need for promoting Internet security awareness programme for Nigeria that would assist in creating an Internet-secure culture in Nigeria among all of the users of the Internet. The focus of the research is improving security culture by regularly promoting Internet security awareness. This involves making sure Internet users receive awareness training when making use of the Internet, applying contextual training relevant to the actions they are carrying out (see Chapter 9).

This research also advocates that private institutions that practice self-regulation should have a larger part in encouraging the use of the awareness programme. Telecommunication organisations could play a part in the application process as many Nigerian Internet users make use of mobile phones. Financial institutions could provide awareness for their customers on Internet banking security issues on their Internet banking websites. This could

potentially reduce identity theft and fraud issues and at the same time improve their overall services to their customers.

The research also briefly explored encouraging the use of the awareness programme to improve users Internet security awareness by giving incentives such as free data storage space. The rationale behind this approach is that the cost of the incentives would be covered because the current self-regulation techniques being practiced by organisations would be more effective if they improve Internet users' attitude towards privacy and Internet security and encourage the practicing of self-protection techniques.

11.2 Research Implications

The research provides significant contributions to knowledge by discovering the issues in Nigeria's e-commerce privacy and security and defining strategies, which help in developing solutions. The research establishes the existence of the problem and its extent, identifying the factors, which affect privacy and data protection, including the cultural and country-specific factors, and it then defines a framework containing recommendations for self-regulation and promoting contextual awareness programmes through security warnings as a solution.

The framework will help the Nigerian organisations to enhance people's awareness of the Internet threats through a set of useful recommendations and effective methods tailored to the Nigerian context. The research is beneficial for the groups, such as the Nigerian Government, citizens and organisations responsible for ensuring Internet security to enable them to help protect the security and privacy of Nigerian Internet users and, ultimately, develop e-commerce and Internet penetration and trust. In addition, many of the research ideas would be useful for research scholars, and researchers on Internet privacy, security and awareness, especially in those countries with background and culture similar to Nigeria, such as other

African and developing countries.

In terms of implications for practice, the research offers a guide for the adoption process, which will be useful for those involved in ensuring the Internet privacy and security, and to inspire online businesses and Internet users to employ good privacy and security practices. The recommendations have been validated and were considered to be very useful by both Nigerian IT security experts and by general Nigerian Internet users, hence it is believed the framework can be used throughout Nigeria and this could also be extended to other developing countries, especially those with a similar culture in Africa.

11.3 Research Contributions

This research has contributed to the existing body of literature by filling the gaps of previous studies regarding Internet privacy, security and data protection in developing countries, with particular emphasis on Nigeria. The research has empirically identified key factors affecting the data protection and privacy and factors affecting the adoption of different existing data protection approaches.

There is a lack of scholarly articles on the privacy practices of Nigerian websites. Therefore, this study adds to the existing body of literature and makes specific contributions by providing insights on the privacy practices of Nigerian websites as well as being able to identify the areas that needs more focus.

It was observed that although many studies have indicated a problem with the current state of the privacy and data protection in Nigeria, none has put forward and verified strategies or guidelines for resolving the various issues. Hence, this research has put together strategies in the form of a framework that can assist the Nigerian government and other relevant

organisations, such as the banks and ISPs, as well as online businesses and Internet users, to resolve the problems of Internet privacy and security.

In other words, creating a framework to aid the successful adoption and effective penetration of e-commerce through Internet privacy and data protection constitutes the central contribution of this research. This research has also made a novel contribution as it has identified the major stakeholders who could take responsibility for improving Internet privacy and security, particularly in Nigeria, which has not been identified in previous research.

The framework that has been developed in this research can be applied by other researchers considering research in similar areas such as the adoption or use of the framework in other developing countries. The framework will generally assist decision makers to set a strategic action plan for the further overall development of e-commerce in developing countries.

The research was able to establish that there are no effective government solutions to the Internet privacy and security issue in Nigeria and, because of Nigeria's unique factors, involving the government fully or solely in solutions may not be effective.

Insight was also given to Nigerian Internet users' perception of data protection and personal information privacy. Although there is high cybercrime in Nigeria, Internet users have limited awareness and interest in these issues. There are many factors that affect privacy and data protection in Nigeria and lack of awareness is one of the main factors.

The research findings suggest that factors which affect the adoption and effective use of data protection approaches can be different in each country and, thus, possible solutions should incorporate these cultural and country-specific factors in order for them to be effective.

The research makes a methodological contribution by using different data collection methods to assist in increasing the validity of the research findings. The research made use of data from semi-structured interviews, questionnaires, and the review of documents such as policy documents as primary sources of evidence whilst secondary sources of evidence comprised mainly journals, conference papers, text books and organisations' websites.

Methodologically, the research employed a questionnaire survey, qualitative interviews, observations and review of documents as data collection tools. This means that the research employed both qualitative and quantitative approaches in order to provide in-depth information about the subject.

11.4 Research Limitations

One limitation of this research is the fact that the collection of data depended mainly on the level of access that was granted to the researcher, especially during the interviews and questionnaires. Therefore, the participants could have hidden some vital information from the researcher, which could possibly have affected the research outcome, without the researcher's knowledge.

Although the main data collection technique used to understand the Internet users' perception of privacy was via a questionnaire, the researcher went a step further to get more insight on the participants' responses via semi-structured interviews. The participants' reluctance to participate in interviews and surveys was a further constraint. However, the researcher tried to take steps to encourage people to participate, for instance by refraining from tape recording the interviews and assuring their confidentiality.

The study was limited to Nigeria as an example of a developing country. It is the researcher's belief that although the research was limited to Nigeria, nevertheless, some of the research

findings are likely to be similar to those in other developing countries. However, the research findings cannot be generalised without additional research. Similarly, despite the fact that issues concerning Nigeria are homogeneous, it is still difficult to generalise Nigeria's results to other developing countries of the world without conducting additional research.

Due to the limited resources, the researcher was not able to fully implement part of the proposed awareness programme and recommendations in reality. However, using a prototype and the opinion of experts from a range of private and government organisations gave a useful, if limited, test of the recommendations.

11.5 Recommendations for Further Research

The findings of this research and the research limitations have resulted in the identification of potential future research directions for investigation. The recommendations for further research as a result of this study are:

More research is needed to further validate the findings, in order to increase the generalisation of the results in different areas within Africa and over different developing countries round the world. Re-testing the research findings and the recommendations in other regions within Africa especially, will help to determine whether the recommendations would have the same impact or would be less significant in other areas.

The recommendations in this thesis and the awareness framework developed have been tested within the time constraints of a PhD project. The research needs to continue over a longer period to see the effects of the recommendations and framework being put into practice in Nigeria. This research would require the cooperation of the government and other institutions to apply the recommendations and awareness framework so the effects can be studied, which, clearly, is well beyond the scope of a PhD research project.

This research has revealed that country-specific considerations are important factors affecting privacy and data protection in Nigeria. It would be interesting to find if there are other country-specific factors and whether these affect some other developing countries more than others. Comparative studies could be conducted in other developing countries, for example Ghana or India, to determine differences in the context of developing countries. Also, a more detailed comparison should be been made with a developed country, such as the United Kingdom. For instance, comparing country specific factors and the applicability of the recommendations in other countries.

The recommendations and awareness framework developed has been specifically designed for Nigeria. However, it is likely that many of the recommendations and parts of the framework would be applicable in other developing countries. The various different components of the framework and recommendations could be tested in a number of different countries to discover what parts of the framework work well in different countries and this would also help identify the conditions that would make each component and recommendation applicable. This further research would then help other countries decide how to apply the recommendations and framework themselves.

11.6 The Success of this Research Project

This research has derived a framework of recommendations and awareness training that has been shown to be both applicable and likely to be very effective in Nigeria. Some of the findings of the research have already been published (see the publications list) and there are plans to publish further papers on the research in reputable journals. This will place the research in the public domain, where it is hoped it will be read and then applied in Nigeria and in similar developing countries, and will become the basis for the further research suggested.

Appendix A: Survey (questionnaire)

A1 First version of questionnaire

Aim: This survey will analyse the public understanding and knowledge of data protection and Internet privacy in Nigeria. The questionnaire contains 26 simple questions.

Q1 Gender

- ❍ Male
- ❍ Female

Q2 Age

- ❍ >20
- ❍ 20-29
- ❍ 30-39
- ❍ 40-49
- ❍ 50 +

Q3 Where do you currently live

- ❍ Nigeria
- ❍ Other African countries
- ❍ Outside Africa

Q4 If the answer for above is outside Africa please specify

Q5 Occupation

- Student
- Job in private sector
- Job in public sector
- Unemployed
- Self employed
- Others

Q6 Educational Qualifications

- PhD
- Masters degree
- Bachelors degree
- Undergraduate
- School Certification
- Primary School
- Others

Q7 Do you buy things or perform transactions online?

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q8 Does it bothers you when Websites ask for personal information?

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q9 Which of the following information is personal to you that you would NOT like to share when making a transaction online?

	Always feel comfortable (1)	Sometimes feel comfortable (2)	Rarely feel comfortable (3)	Never feel comfortable (4)
Annual Income	❍	❍	❍	❍
Age	❍	❍	❍	❍
Bank account details	❍	❍	❍	❍
Credit/Debit card details	❍	❍	❍	❍
Email address	❍	❍	❍	❍
Facebook address	❍	❍	❍	❍
Full name	❍	❍	❍	❍
Gender	❍	❍	❍	❍
Health and medical history	❍	❍	❍	❍
Home address	❍	❍	❍	❍
Land line/mobile phone number	❍	❍	❍	❍
Photograph	❍	❍	❍	❍

Martial Status	❍	❍	❍	❍
Occupation	❍	❍	❍	❍
Passport number	❍	❍	❍	❍
Religion	❍	❍	❍	❍
All of the above	❍	❍	❍	❍

Q10 What is your preferable mode of online payment?

- ❍ Credit/debit card
- ❍ Bank Transfer
- ❍ Pay on Delivery
- ❍ Others

Q11 I am very concerned about the threats to personal privacy today

- ❍ Strongly agree
- ❍ Agree
- ❍ Neither Agree nor Disagree
- ❍ Disagree
- ❍ Strongly Disagree

Q12 Websites can hinder privacy by collecting personal information

- ❍ Strongly agree
- ❍ Agree
- ❍ Neither Agree nor Disagree
- ❍ Disagree
- ❍ Strongly Disagree

Q13 Do you read the privacy policy or terms of conditions of a website before giving your personal information?

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q14 Do you verify authenticity of a website before giving your personal information?

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q15 Have you ever wondered what happens to the personal data provided on a website?

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q16 Have you ever wondered what happens to your data when you close your account on a website?

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q17 Which of the following privacy enhancing techniques are you aware of?

- ❑ Deleting cookies
- ❑ Altering browser settings
- ❑ Providing false information on websites
- ❑ None
- ❑ Others

If others is selected, Then Skip To 16. Please specify others

Q18 Please specify others

Q19 Are you aware of spam emails or text messages

- ❍ Yes
- ❍ Not sure
- ❍ No

Q20 Do you receive spam emails or text messages

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q21 Does getting spam emails and/or text messages from third party organisations with which you have never shared your data bother you

- ❍ Always
- ❍ Very Often
- ❍ Occasionally
- ❍ Never

Q22 Are you aware of identity theft and the repercussions

- ❍ Yes
- ❍ Not sure
- ❍ No

If Yes Is Selected, Then Skip To How did you gain awareness If No Is Selected, Then Skip To What do you do in the case your perso...

Q23 How did you gain awareness?

- ❍ Training
- ❍ Online
- ❍ School
- ❍ Media
- ❍ Others

Q24 Do you think it is possible for somebody to steal your identity with information you have provided on websites

- ❍ Yes
- ❍ Not sure
- ❍ No

Q25 What do you do in the case your personal data being misused

- ❍ Send a complain to the defaulting organisation
- ❍ Report straight to the authorities
- ❍ Do nothing

Q26 Government can generally be trusted to look after privacy interests.

- ❍ Strongly agree
- ❍ Agree
- ❍ Neither Agree nor Disagree
- ❍ Disagree
- ❍ Strongly Disagree

A2 Questionnaire final version (after pilot-test)

Covering letter

Dear Sir or Madam,

I am a PhD student at Loughborough University in the UK and I am doing my research on e-commerce privacy and data protection in Nigeria.

I have designed a questionnaire to see how aware people are information privacy, data protection and self-protection techniques. This questionnaire is tailored only for Nigerian Internet users.

The questionnaire will take no more than 5 minutes of your time to complete. I really appreciate your contribution. It is intended to use the results in developing recommendations that will improve the Internet privacy and security in Nigeria.

I assure you that all responses will be confidential and will only be used for the purpose of the research.

Thank you for your assistance

Perception of Data Protection and Privacy in Nigeria

Q1 Gender

- ❍ Male
- ❍ Female

Q2 Age

- ❍ <20
- ❍ 20-29
- ❍ 30-39
- ❍ 40-49
- ❍ 50 +

Q3 Nationality

- ❍ Nigeria
- ❍ Other African Country
- ❍ Outside Africa

Q4 Where do you currently live?

- ❍ Nigeria
- ❍ Other African countries
- ❍ Outside Africa

Q5 Occupation

- ❍ Student
- ❍ Job in private sector
- ❍ Job in public sector
- ❍ Unemployed
- ❍ Self employed
- ❍ Others

Q6 Education Qualification

- ❍ PhD
- ❍ Masters degree
- ❍ Bachelors degree
- ❍ Undergraduate
- ❍ School Certification
- ❍ Primary School
- ❍ Others

Q7 How often do you use the Internet?

- ❍ Everyday/Almost everyday
- ❍ Two or three times a week
- ❍ About once a week
- ❍ Two to three times a month
- ❍ Less often
- ❍ No internet access
- ❍ Never

Q8 Do you buy things or perform transactions online?

- ❍ Always
- ❍ Most of the Time
- ❍ Sometimes
- ❍ Rarely

❍ Never

Q9 For the following statement, could you please indicate whether you tend to agree or disagree?

	Agree	Disagree	Not sure
Disclosing Personal Information is increasing Part of modern life	❍	❍	❍
There is no alternative than to disclose personal information if one wants to obtain product and services	❍	❍	❍
Disclosing personal information is not a big issue	❍	❍	❍
I don't mind disclosing personal information in return for free services online	❍	❍	❍
I feel obliged to disclose Personal	❍	❍	❍

Information on the Internet			

Q10 Which of the following information is personal to you would feel uncomfortable sharing online? (you can chose more than one)

- ❑ Financial Information (bank account details, credit/debit card details, salary)
- ❑ Health/Medical Information
- ❑ Passport Number
- ❑ Home address
- ❑ Mobile/landline number
- ❑ Photograph
- ❑ Full name
- ❑ Email address
- ❑ Facebook address
- ❑ Age
- ❑ Marital status
- ❑ Religion
- ❑ Gender
- ❑ Occupation

Q11 How concerned are you when website ask for personal information?

- ❍ Very concerned
- ❍ Fairly Concerned
- ❍ Not concerned
- ❍ Don't know

Q12 What is your preferable mode of online payment?

- ❍ Credit/debit card
- ❍ Bank Transfer
- ❍ Pay on Delivery
- ❍ Others

Q13 What is the most important reason why you disclose personal information when shopping online? (You can choose more than one)

- ❑ To access service
- ❑ To benefit from personalised offers
- ❑ To receive money or price reductions
- ❑ To save time on next visit
- ❑ For fun
- ❑ Don't know

Q14 According to you, what are the most important risks connected with disclosure of your personal information to buy goods or services via the Internet? (You can choose more than one)

- ❑ Your information being used without your knowledge
- ❑ Being a victim of fraud
- ❑ Your information shared with third parties without your knowledge
- ❑ Risk of identity theft
- ❑ Your personal safety being at risk

- ❑ Your reputation being at risk
- ❑ Discrimination
- ❑ None
- ❑ Don't know

Q15 Thinking about website privacy statements on the Internet, which of the following sentences best describes your situation?

- ❍ You usually read and understand them
- ❍ You usually read but do not understand them
- ❍ You don’t usually read them
- ❍ You do not know where to find them
- ❍ you totally ignore them
- ❍ Don't know

Q16 Does reading online privacy statement change your behaviour online?

- ❍ Yes
- ❍ No
- ❍ Don't know

Q17 Which of the following privacy enhancing techniques are you aware of? (you can choose more than one)

- ❑ Deleting cookies
- ❑ Altering browser settings

- ❑ Providing false information on websites
- ❑ Antivirus
- ❑ Check for https on the website
- ❑ Check for security logo or web seal
- ❑ None
- ❑ Others

Q18 Please specify others

Q19 Have you ever wondered what happens to the personal data provided on a website

- ❍ Always
- ❍ Most of the Time
- ❍ Sometimes
- ❍ Rarely
- ❍ Never

Q20 Are you aware of spam emails or text messages?

- ❍ Yes
- ❍ Not sure
- ❍ No

Q21 Do you receive spam emails or text messages?

- ❍ Always
- ❍ Most of the Time
- ❍ Sometimes
- ❍ Rarely
- ❍ Never

Q22 Does getting spam emails and/or text messages from third party organisations with which you have never shared your data bother you

- ❍ Always bothered
- ❍ Sometimes bothered
- ❍ Never bothered
- ❍ Don't know

Q23 Have you heard about or experienced issues in relation to data losses and identity theft? (You can choose more than one)

- ❑ Yes through the media (television, radio, newspaper, Internet)
- ❑ Yes, through word of mouth
- ❑ Yes, it affected someone I know
- ❑ Yes, It affected me directly
- ❑ No
- ❑ Don't know

Q24 Do you think it is possible for somebody to steal your identity with information you have provided on websites?

- Yes
- Not sure
- No

Q25 Who do you think should be responsible for protecting your information collected and stored in the website?

- You (you need to take care of your information)
- Websites (they need to ensure their customers information is protected)
- Government or public authorities (they need to ensure the citizens information are protected)
- Third party organisations (banks)
- Don't know

Q26 What do you do in the case your personal data being misused?

- Send a complain to the defaulting website
- Report straight to the authorities
- Do nothing

Q27 To what extent do you trust the following institutions to protect your personal information?

	Total trust	Somewhat trust	Do not trust	Don't know

E-commerce websites	❍	❍	❍	❍
Banking and financial institution	❍	❍	❍	❍
Government or public institution	❍	❍	❍	❍

A3 Questionnaire results

In total 220 participants have participated in the survey as shown below

Analysis of Questionnaire

Trust in e-commerce companies/ Performs transactions online	**Always**	**Most of the time**	**Sometimes**	**Rarely**	**Never**	**Total**
Total trust	10	4	5	8	3	30
Somewhat trust	15	21	46	14	5	101
Do not trust	5	6	9	14	13	47
Total	30	31	60	36	21	178

To find whether there is a relationship between respondents who trust e-commerce websites and those who are comfortable performing online transactions, Chi-squared test was applied as follows:

$\chi 2$ was calculated using the following formula:

Chi-squared $\chi 2 = 36.3$

Degrees of freedom= 8

P-value= .000015 at $p < .05$

Where:

H0= There is no relation between the two responses

H1= There is relation between the two responses

It was concluded that there is a relationship between respondents who trust e-commerce websites and those who are comfortable performing online transactions.

Comfortable disclosing personal information/Performs transactions online	Always	Most of the time	Sometimes	Rarely	Never	Total
Always	27	10	21	8	8	74
Most of the time	5	10	22	12	4	53
Sometimes	4	11	11	14	5	45
Rarely	1	3	6	4	3	17
Never	1	0	1	4	4	10
Total	38	34	61	42	24	199

The chi-squared test shows also a clear relationship between the respondents wanting to purchase online and disclosing personal information

Chi-squared $\chi 2 = 42.37$

Degrees of freedom= 16

P-value= .00007 at $p < .05$

The table below is a chi-squared test that shows clearly a relation between levels of awareness with age

Age/ awareness of privacy enhancing techniques	
Chi-square	52.98
Degrees of freedom	28
P-Value	.000007

A4 interview Questions

10 of the questionnaire respondents were chosen at random and interviewed face-to-face by semi- structured interview containing the following questions:

1. Do you usually feel comfortable providing your personal information when performing transactions online?
2. Which information are you least comfortable providing
3. Do you ever read a website's policies?
4. If no, why?
5. If yes, why?
6. Is the Nigerian government reliable enough to handle privacy issues in Nigeria
7. Which private institution do you think should be responsible for protecting customers' information?

Appendix B Interviews

This section provides the face-to-face, semi-structured interviews questions held with experts in Nigeria in relation to e-commerce privacy and data protection and the recommendations made in the study.

B1 Cover letter for interviews

I am a PhD student at Loughborough University, United Kingdom. I am currently conducting research on e-commerce privacy and data protection in Nigerian. The purpose of the research is to better understand the current privacy and data protection issues in Nigeria and make applicable recommendations.

I have identified some recommendations that would improve privacy and data protection risk in Nigeria. I would be very grateful if you could participate in an interview regarding this research to understand the current situations and attitudes in Nigeria and validate the recommendations of this research.

I assure you all responses will be confidential and kept strictly private.

Yours faithfully,

Tiwalade Adelola (PhD student)

B3 Interview questions

Questions for e-commerce employees

1. Can you briefly describe your company's history?
2. What data protection methods are currently being implemented in your company?
3. Are there any government regulations in place to protect your customers' personal information?
4. Which organisation handles customers' disputes?
5. Based on the information I have provided about the research and my findings, what are your views on the recommendations made
6. Are there any limitations that might be experienced if they were implemented?
7. Do you have any further suggestions or comments?

Questions for Bank employees

1. What are the current services you provide for e-commerce websites?
2. Can you provide more details on how you handle privacy and security related disputes?
3. Does the government get involved in dispute resolutions
4. Based on the information I have provided about the research and my findings, what are your views on the recommendations made
5. Are there any limitations that might be experienced if they were implemented?
6. Do you have any further suggestions or comments?

Questions for Government officials

1. Are there any data protection legislations being implemented currently and/or later in the future?

2. Can you comment on the current legislations in place and how effective they are in addressing data protection?
3. What other initiatives are in place to ensure Nigerian Internet users' personal information are protected?
4. Based on the information I have provided about the research and my findings, what are your views on the recommendations made
5. Are there any limitations that might be experienced if they were implemented?
6. Do you have any further suggestions or comments?

Appendix C Validation of Awareness Training Method

This section describes the process involved in validation the awareness training method.

C1 Validation by Internet users (questionnaire)

Covering letter

Dear Sir or Madam,

I am a PhD student at Loughborough University in the UK and I am doing my research on e-commerce privacy and data protection in Nigeria. Based on the research findings, I have developed an awareness training method that utilises the usual security web pages and contextual training to improve the way awareness programmes are delivered.

I have included a link to a prototype website with detailed information on how to proceed with the process. I have also attached a questionnaire to gather your views on the recommended training method.

The whole will take no more than 10 minutes of your time to complete. I really appreciate your contribution. It is intended to use the results establish the relevance and applicability of the method.

I assure you that all responses will be confidential and will only be used for the purpose of the research.

Thank you for your assistance.

Validation of Awareness Training method (Questionnaire)

Q1 Gender

- ❍ Male
- ❍ Female

Q2 Age

- ❍
- ❍ 20-29
- ❍ 30-39
- ❍ 40-49
- ❍ 50 +

Q3 Occupation

- ❍ Student
- ❍ Job in private sector
- ❍ Job in public sector
- ❍ Unemployed
- ❍ Self employed
- ❍ Others, please specify _____

Q4 Education Qualification completed

- ❍ PhD
- ❍ Masters degree
- ❍ Bachelors degree
- ❍ Undergraduate
- ❍ School Certification
- ❍ Primary School
- ❍ Others

Q5 How often do you use the internet?

- ❍ Everyday/Almost everyday
- ❍ Two or three times a week
- ❍ About once a week
- ❍ Two to three times a month
- ❍ Less often
- ❍ No internet access
- ❍ Never

Q6 Which of the following do you have in place in order to protect your computer and electronic data? (you can chose more than one)

- ❑ Antivirus Software
- ❑ Firewall
- ❑ Anti-spam filter
- ❑ Good Password
- ❑ Regular software updates

Q7 Did you notice/read the threat prompt?

- ❍ Yes
- ❍ No

Q8 Did you follow the awareness programme link provided?

- ❍ Yes
- ❍ No

If Yes Is Selected, Then Skip To How much of the programme did you go ...If No Is Selected, Then Skip To Why didn't you visit the link?

Q9 Why didn't you visit the link?

- ❍ Didn't understand the prompt
- ❍ Uninterested
- ❍ Already know about the issue
- ❍ Could easily visit another website
- ❍ Others, please specify _____

Display This Question:

Did you follow the awareness programme link provided? If Yes Is Selected:

Q10 How much of the programme did you go through?

- ❍ All of it
- ❍ Most of it
- ❍ Just a little bit
- ❍ Left after the first page

Q11 This is an effective way of enforcing cyber-security awareness

- ❍ Strongly agree
- ❍ Agree
- ❍ Neither agree nor disagree
- ❍ Disagree
- ❍ Strongly agree

Q12 Would you visit the link if there is an incentive, for example extra Internet data or a gift card?

- ❍ Yes
- ❍ No

Q13, Which Incentive would you, prefer?

- ❍ Internet data
- ❍ Gift card
- ❍ free antivirus software
- ❍ Free movie tickets
- ❍ others, please specify _____

C2 Validation by Internet users (focus group)

Covering letter

Dear Sir or Madam,

I am a PhD student at Loughborough University in the UK and I am doing my research on e-commerce privacy and data protection in Nigeria. Based on the research findings, I have developed an awareness training method that utilises the usual security web pages and contextual training to improve the way awareness programmes are delivered.

You are cordially invited to take part in a focus group to discuss your views and suggestions on the recommended awareness training method. I have included a link to a prototype website with detailed information on how to proceed with the process.

I really appreciate your contribution. It is intended to use the results establish the relevance and applicability of the method. I assure you that all responses will be confidential and will only be used for the purpose of the research.

Thank you for your assistance.

Focus group questions

1. Have you ever been exposed to any awareness-training programme?
2. What are your opinions about the presented training method?
3. Do you think you this method could help raise awareness in the general population?

4. Do you think this training method is feasible and can be implemented by relevant Private institutions?
5. Are there any limitations that might be experienced if they were implemented?
6. Do you have any further suggestions or comments?

C3 Analysis of Validation results

In total 136 participants have participated in the validation process:

Analysis of Results

An analysis was done to find out if there is a relation between the participants that thought the programme was an effective way of promoting cyber-security awareness and those that went through the programme.

Thought training method was effective/ How much of the programme did you go through	
Chi-square	31.94
Degrees of freedom	12
P-Value	.000008

C4 Validation by experts

Cover letter

I am a PhD student at Loughborough University, United Kingdom. I am currently conducting research on e-commerce privacy and data protection in Nigerian. I have

developed an awareness training method that utilises the usual security web pages and contextual training to improve the way awareness programmes are delivered.

You are cordially invited to take part in an open-ended survey to discuss your views and suggestions on the recommended awareness training method. I have included a link to a prototype website with detailed information on how to proceed with the process.

I really appreciate your contribution. It is intended to use the results establish the relevance and applicability of the method. I assure you that all responses will be confidential and will only be used for the purpose of the research.

Thank you for your assistance.

Validation of Awareness Training method (Questionnaire)

Q1 Gender

- ❍ Male
- ❍ Female

Q2 Age

- ❍ <20
- ❍ 20-29
- ❍ 30-39
- ❍ 40-49
- ❍ 50 +

Q3 Type of organisation do you work in?

Q4 Position in Organisation you work in

Q5 Education Qualification completed

- ❍ PhD
- ❍ Masters degree
- ❍ Bachelors degree
- ❍ Undergraduate
- ❍ School Certification
- ❍ Primary School
- ❍ Others

Q6 Did you notice/read the threat prompt?

- ❍ Yes
- ❍ No

Q7 Did you follow the awareness programme link provided?

- ❍ Yes
- ❍ No

If Yes Is Selected, Then Skip To How much of the programme did you go ...If No Is Selected, Then Skip To Why didn't you visit the link?

Q8 Why didn't you visit the link?

- ❍ Didn't understand the prompt
- ❍ Uninterested
- ❍ Already know about the issue
- ❍ Could easily visit another website
- ❍ others, please specify _____

Display This Question:

Did you follow the awareness programme link provided? If Yes Is Selected:

Q9 How much of the programme did you go through?

- ❍ All of it
- ❍ Most of it
- ❍ Just a little bit
- ❍ Left after the first page

Q10 Please briefly describe any current cyber-security awareness programme practices being used by your organisation

Q11 Could this be an effective way of promoting cyber-security awareness for your organisation's customers'

Q12 Do you think this awareness programme can be implemented by your organisation?

- Yes
- Not sure
- No

Q13 What Incentives could your organisation provide for your customers to promote cyber-security awareness

Q14 Please discuss any comments or suggestions you have in relation to the programme

Appendix D: Analysis of Nigerian websites

This section shows a list of the websites used for the analysis of their privacy policies

D1 Nigerian websites

E-commerce site	URL
Mauxy	https://www.mauxy.com/
Chrisvicmall	https://chrisvicmall.com/
Numart	https://numartng.com/
Quickbuy	http://quickbuyservices.com/
Bensultd	http://bensultd.com/
Dream care	http://www.dreamcare.com.ng/
Topdown deals	http://www.topdowngames.com.ng/
Buyright	http://www.buyright.biz/
Traclist	http://traclist.com/
Adam and eve	http://adameveshop.com/
Komo online	http://www.komoonline.com/
Eboizi	http://eboizi.com/
Viewden	http://www.viewden.com/store/
1500	http://www.1500naira.com
Easy shop	http://www.easyshop.com.ng/
3al	https://www.3al.com/
Webmall	https://www.webmallng.com/
Walahi	http://walahi.com/
Timetell	http://www.time-tellng.com/
Flo shop	http://flocargo.com/
Smartbuy	http://www.smartbuy.ng/
Shopaholic	https://shopaholicng.com/
Scuup	https://scuupng.smemarkethub.com/
Procure it Nigeria	http://www.procureitnigeria.com/
Costumes galore	http://costumesgalore.com.ng/

Osarmoire	http://www.osarmoire.com/
Naija shop	http://naijashop.com.ng/
My gadgets mall	http://www.mygadgetsmall.com/
Myboolah	http://myboolah.com/
Shop and mall	http://www.mallforafrica.com/shop
Mizzy b	https://mizzybshoesonline.com.
Manna stores	http://www.mannastores.com/
Laternabooks	https://laternabooks.com/
Irqa books	http://www.iqrabooks.com.ng/
Gafunk	http://gafunk.info/gafunknew/
Emart	https://www.emartnigeria.com/
Depearl	http://www.depearl.com/
Dafun	http://dafunshop.com/
Circuit atlantic	http://www.circuitatlantic.com/
Payporte	https://www.payporte.com/
Mystore	https://www.mystore.com.ng/
Mrp	https://www.mrp.com/en_ng/
Supermart	https://www.supermart.ng/
Wakanow	https://www.wakanow.co.uk/
Kaymu	http://www.kaymu.com/
Dealmayor	http://www.mobofree.com/nigeria/
Kinkimall	https://www. Kinkimall.ng
Swiftng	http://www.swiftng.com/
Oja shop	http://ojabuy.com/seller/ojashop/
Parktel online	https://parktelonline.com/
Kara.com	http://www.kara.com.ng/
Gloo.ng	https://www.gloo.ng/
Slot limited	https://slot.ng/
Dealdey	https://www.dealdey.com/
Buynigeriaonline	http://buynigeriaonline.com

Buycorrect	http://www.buycorrect.com/
Shoptomydoor.	http://www.shoptomydoor.com/
3bids	http://www 3bids.com
Mauxy	https://www.mauxy.com/
The primemall	https://theprimemall.com/
Ozyet	https://www.myguidenigeria.com/shopping/ozyet
Kudi	https://kudi.com/
Jumia	https://www.jumia.com.ng/
Konga	https://www.konga.com/
Egole	http://egoleshopping.com/

Bibliography

Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology,* 33(3), pp. 237-248.

Acquaye, N. (2011) *Data protection bill withdrawn.* Available at: http://www.biztechafrica.com/article/data-protection-bill-%20withdrawn/933/#.U7qt1vldV8E (Accessed: 04/07/2015).

Adewole, K.S., Olayemi, R.T. and Isiaka, R.M. (2011) 'An inquiry into the awareness level of cyber security policy and measures in Nigeria', 1(7), pp. 91.

Adkinson, W.F., Eisenach, J.A. and Lenard, T.M. (2002) 'Privacy online: A report on the information practices and policies of commercial web sites', *Progress and Freedom Foundation, Washington DC,* .

Akanbi, B. and Akanbi, C. (2012) 'Bridging the digital divide and the impact on poverty in Nigeria', *Computing, Information Systems & Development Informatics,* 3(4), pp. 83-85.

Akinsuyi, F. (2010) *Data Protection for Nigeria, the time is now.* Available at: ttp://www.datalaws.com/common/pdf/Article02.pdf (Accessed: 03/02/2015).

Akomolede, T. (2008) 'Contemporary Legal Issues in Electronic Commerce in Nigeria'(2008)', *Potchefstroom Electronic Law Journal,* 11, pp. 1, 12-13.

Altinay, L., Paraskevas, A. and Jang, S.S. (2015) *Planning research in hospitality and tourism.* Routledge.

Antón, A., Earp, J.B. and Reese, A. (2002) *Analyzing website privacy requirements using a privacy goal taxonomy.* IEEE, pp. 23.

Anttila, J., Savola, R., Kajava, J., Lindfors, J. and Röning, J. (2007) *Fulfilling the needs for information security awareness and learning in information society.*

ASYCUDA (2017) *Glossary of Custom Terms.* Available at: https://asycuda.org/cuglossa.asp?term=developing&submit1=Search (Accessed: 07/09/2017).

Australian Information Commissioner (2013) *Guidelines for recognising external dispute resolution schemes under s 35A of the Privacy Act 1988.* Office of the Australian Information Commissioner, .

Barber, R. (2001) 'Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated.', *Computer Fraud & Security,* 2001(3), pp. 9-12.

Bart, Y., Shankar, V., Sultan, F. and Urban, G.L. (2005) 'Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study', *Journal of Marketing,* 69(4), pp. 133-152.

Basit, T. (2003) 'Manual or electronic? The role of coding in qualitative data analysis', *Educational research,* 45(2), pp. 143-154.

Bassey, D.E., Okoro, R., Okon, B. and Eyime, E. (2016) 'Broadband–Infrastructural Deficit and ICT Growth Potentials in Cross River State, Nigeria', *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE),* 4(5), pp. 8465-8476.

Bellotti, V. (1997) *Design for privacy in multimedia computing and communications environments.* MIT Press, pp. 63.

Berelson, B. (1952) 'Content analysis in communications research', .

Bergström, A. (2015) 'Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses', *Computers in Human Behavior,* 53, pp. 419-426.

Birnhack, M. and Elkin-Koren, N. (2009) 'Does law matter online? Empirical evidence on privacy law compliance', .

Boniface, K.A., Michael, K.A. and Victor, K.O. (2015) 'Cyber Security in Nigeria: A Collaboration between Communities and Professionals', *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering,* 9(5), pp. 1344-1348.

Borena, B., Belanger, F. and Egigu, D. (2015) *Information Privacy Protection Practices in Africa: A Review through the Lens of Critical Social Theory.* IEEE, pp. 3490.

Boritz, J.E. and No, W.G. (2011) 'E-commerce and privacy: Exploring what we know and opportunities for future discovery', *Journal of Information Systems,* 25(2), pp. 11-45.

Bourque, L. (2003) *How to conduct self-administered and mail surveys.* Sage.

Boyatzis, R.E. (1998) *Transforming qualitative information: Thematic analysis and code development.* Sage.

Bradbury, D. (2012) 'The dangers of badly formed websites', *Computer Fraud & Security,* 2012(1), pp. 12-14.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative research in psychology,* 3(2), pp. 77-101.

Britten, N. (1995) 'Qualitative interviews in medical research', *BMJ (Clinical research ed.),* 311(6999), pp. 251-253.

Broadcasting Board of Governors (2014) 'Contemporary Media Use in Nigeria', .

Brookman, J. (2015) 'Protecting Privacy in an Era of Weakening Regulation', *Harv.L.& Pol'y Rev.,* 9, pp. 355.

Bryman, A. (2015) *Social research methods.* Oxford university press.

Bryman, A. (2006) 'Integrating quantitative and qualitative research: how is it done?', *Qualitative research,* 6(1), pp. 97-113.

Byström, K. (1999) *Information seekers in context: an analysis of the'doer'in INSU studies.* Taylor Graham Publishing, pp. 82.

Carr, N. (2010) *Tracking is an assault on liberty, with real dangers.* Available at: https://www.wsj.com/articles/SB10001424052748703748904575411682714389888 (Accessed:19/02/2016) .

Cassell, C. and Symon, G. (2004) *Essential guide to qualitative methods in organizational research.* Sage.

Cate, F.H. and Mayer-Schönberger, V. (2013) 'Notice and consent in a world of Big Data', *International Data Privacy Law,* 3(2), pp. 67-73.

Cavoukian, A. and Crompton, M. (2000) 'Web Seals: A Review of Online Privacy Programs', .

CDC (2013) *CDC's e-learning essentials; a guide for creating quality electronic learning.*

Central Intelligence Agency (2015) *The world fact book.* Available at: https://www.cia.gov/library/publications/resources/the-world-factbook/geos/ni.html (Accessed: 08/02/2016).

Central Intelligence Agency (CIA) (2017) *The World Fact Book.* Available at: https://www.cia.gov/library/publications/the-world-factbook/geos/ni.html (Accessed: 27/08/2017) .

Chen, T., Jeng, F. and Liu, Y. (2006) *Hacking tricks toward security on network environments.* IEEE, pp. 442.

Chiejina, C. and Olamide, S.E. (2014) 'Investigating the Significance of the 'Pay on Delivery' Option in the Emerging Prosperity of the Nigerian e-commerce sector', *Journal of Marketing and Management,* 5(1), pp. 120.

CIA (2015) *The world fact book: Nigeria.* Available at: https://www.cia.gov/library/publications/the-world-factbook/geos/ni.html (Accessed:08/02/2016) .

Collis, J. and Hussey, R. (2003) 'Business research: A practical guide for postgraduate and undergraduate students',

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007) 'A video game for cyber security training and awareness', *Computers & Security,* 26(1), pp. 63-72.

Cottrell, L. (2014a) *Internet Anonymizers.* Available at: http://www.livinginternet.com/i/is_anon_work.htm (Accessed: 09/08/2015).

Cottrell, L. (2014b) *Remailers.* Available at: http://www.livinginternet.com/i/is_remailers.htm (Accessed: 09/08/2015).

Cox, A., Connolly, S. and Currall, J. (2001) 'Raising information security awareness in the academic setting', *Vine,* 31(2), pp. 11-16.

Creswell, J.W. (2013) *Research design: Qualitative, quantitative, and mixed methods approaches.* Sage publications.

CSEAN (2015) *About CSEAN.* Available at: http://csean.org.ng/about-csean/ (Accessed: 24/08/2015).

Cyr, D. (2014) 'Return visits: a review of how web site design can engender visitor loyalty', *Journal of Information Technology,* 29(1), pp. 1-26.

Darke, P., Shanks, G. and Broadbent, M. (1998) 'Successfully completing case study research: combining rigour, relevance and pragmatism', *Information systems journal,* 8(4), pp. 273-289.

Denscombe, M. (2003) 'The good research guide Maidenhead', .

Desman, M.B. (2003) 'The ten commandments of information security awareness training', *Information Systems Security,* 11(6), pp. 39-44.

Dhamija, R., Tygar, J.D. and Hearst, M. (2006) *Why phishing works.* ACM, pp. 581.

Diallo, A. (2014) *How To Avoid Data Theft When Using Public Wi-Fi.* Available at: http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers- love-public-wi-fi-but-you-can-make-it-safe/ (Accessed: 09/08/2015) .

Dinev, T. and Hart, P. (2006) 'Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use', *E-Service,* 4(3), pp. 25-60.

Dinev, T. and Hu, Q. (2007) 'The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies*', *Journal of the Association for Information Systems,* 8(7), pp. 386.

Du, J.T. and Spink, A. (2011) 'Toward a web search model: Integrating multitasking, cognitive coordination, and cognitive shifts', *Journal of the Association for Information Science and Technology,* 62(8), pp. 1446-1472.

Earp, J.B. and Baumer, D. (2003) 'Innovative web use to learn about consumer behavior and online privacy', *Communications of the ACM,* 46(4), pp. 81-83.

Ehimen, O.R. and Bola, A. (2010) 'Cybercrime in Nigeria', *Business Intelligence Journal-January,* , pp. 93-98.

Elias, P. and Omojola, A. (2015) 'Case study: The challenges of climate change for Lagos, Nigeria', *Current Opinion in Environmental Sustainability,* 13, pp. 74-78.

Eurobarometer (2015) *Special Eurobarometer 431 "Data protection ".* Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf (Accessed: 09/07/2017) .

European commission (2013) *Misuse of your personal data - redress.* Available at: http://ec.europa.eu/justice/data- protection/individuals/misuse-personal-data/index_en.htm. (Accessed:08/05/2015).

European Commission (2009) 'The future of online privacy and data protection', in European Commission (ed.) *Legal analysis of a Single Market for the Information Society*, pp. 2.

Federal Trade Commission (2000) *Privacy online: Fair information practices in the electronic marketplace: A report to congress, May 2000,* .

Ferguson, A.J. (2005) 'Fostering e-mail security awareness: The West Point carronade', *Educase Quarterly,* 28(1), pp. 54-57.

Flinn, S. and Lumsden, J. (2005) 'User perceptions of privacy and security on the web', .

Frees, E.W. (1996) *Data analysis using regression models: the business perspective.* Prentice Hall.

Fulbright, N.R. (2013) 'Global Data Privacy Directory', .

Furman, S.M., Theofanos, M.F., Choong, Y. and Stanton, B. (2011) 'Basing cybersecurity training on user perceptions', *IEEE Security & Privacy,* (2), pp. 40-49.

Furnell, S., Bryant, P. and Phippen, A.D. (2007) 'Assessing the security perceptions of personal Internet users', *Computers & Security,* 26(5), pp. 410-417.

Furnell, S., Gennatou, M. and Dowland, P. (2002) 'A prototype tool for information security awareness and training', *Logistics Information Management,* 15(5/6), pp. 352-357.

Furnell, S., Tsaganidi, V. and Phippen, A. (2008) 'Security beliefs and barriers for novice Internet users', *Computers & Security,* 27(7), pp. 235-240.

Garcia, T. 2013, *How to create a customer security awareness program*, Newsletter edn (unpublished).

Gcaza, N. and von Solms, R. (2017) *Cybersecurity Culture: An Ill-Defined Problem.* Springer, pp. 98.

Gellman, R. (2014) 'Fair information practices: A basic history', *Available at SSRN 2415020,* .

Gellman, R. and Dixon, P. (2011) *Many failures: A brief history of privacy self-regulation in the united states.*

Ghauri, P.N. and Grønhaug, K. (2005) *Research methods in business studies: A practical guide.* Pearson Education.

Hendrix, M., Al-Sherbaz, A. and Victoria, B. (2016) 'Game based cyber security training: are serious games suitable for cyber security training?', *International Journal of Serious Games,* 3(1), pp. 53-61.

Henry, A. (2013) *The Difference Between Antivirus and Anti-Malware (and Which to Use).* Available at: http://lifehacker.com/the-difference-between-antivirus- and-anti-malware-and-1176942277 (Accessed: 24/08/2015) .

Hirsch, D.D. (2011) 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?', .

HM Government (2015) *Learn how to protect yourself, your family and your business.* Available at: https://www.cyberstreetwise.com/ (Accessed: 29/07/2017).

HM Government (2013) *Guiding Principles on Cyber Security.* Available at: https://www.gov.uk/government/publications/cyber-security-guiding-principles (Accessed: 02/08/2015).

Holsti, O.R. (1969) 'Content analysis for the social sciences and humanities', .

Hong, W. and Thong, J.Y. (2013) 'Internet privacy concerns: An integrated conceptualization and four empirical studies', .

Hsieh, H. and Shannon, S.E. (2005) 'Three approaches to qualitative content analysis', *Qualitative health research,* 15(9), pp. 1277-1288.

Huang, D., Rau, P.P. and Salvendy, G. (2010) 'Perception of information security', *Behaviour & Information Technology,* 29(3), pp. 221-232.

Huang, D., Rau, P.P., Salvendy, G., Gao, F. and Zhou, J. (2011) 'Factors affecting perception of information security and their impacts on IT adoption and security practices', *International Journal of Human-Computer Studies,* 69(12), pp. 870-883.

Ibikunle, F. and Eweniyi, O. (2013) 'Approach to cyber security issues in Nigeria: challenges and solution', *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE),* 1(1), pp. 100-110.

Ifinedo, P. (2012) 'Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory', *Computers & Security,* 31(1), pp. 83-95.

Infomation Commissioner's Office (2017) *Enforcement.* Available at: http://ico.org.uk/enforcement. (Accessed: 17/06/2017) .

Information Commissioner's Office (2016) *For the public.* Available at: https://ico.org.uk/for-the-public/ (Accessed: 17/06/2017).

Information Commissioner's office (2014) *Advisory visits.* Available at: http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/advisory_visits. (Accessed: 08/02/2015).

Information Commissioner's Office (2013) *Data Protection Regulatory Action Policy* Available at https://ico.org.uk/media/1853/data-protection-regulatory-action-policy.pdf: (Accessed:08/02/2015) .

Information Commissioner officer (2014) *Complaints performance* Available at: http://ico.org.uk/about_us/performance/complaint_casework_performance. (Accessed: 08/02/2015).

Information Commissioner's Office (2015) *Self assessments.* Available at: http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/self_assessments. (Accessed: 08/02/2015).

Information Resources Management Association (2001) *Managing Information Technology in a Global Economy.* IGI Global.

Ingram, M. (2012) *Welcome to the social network, where your privacy has to be flexible.* Available at: http://www.theglobeandmail.com/technology/on- social-sites-your-privacy-has-to-be-flexible/article4282239/ (Accessed: 15/02/2015).

Internet Live Stats (2017) *Internet Penetration in Africa.* Available at: http://www.internetworldstats.com/stats1.htm (Accessed: 07/08/2017).

Internet Live Stats (2015) *Number of Internet Users (2015) - Internet Live Stats.* Available at: http://www.internetlivestats.com/internet-users/#byregion (Accessed: 8/24/2015).

ITGI (2007) *Cobit Security Baseline: An Information Security Survival Kit.* 2nd edn. Illinois: ITGI.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F. (2007) 'Social phishing', *Communications of the ACM,* 50(10), pp. 94-100.

Jakovljević, M. (2011) 'Information Privacy: The Attitudes and Behaviours of Internet Users', *Oeconomica Jadertina,* 1(1), pp. 12-29.

Jamal, K., Maier, M. and Sunder, S. (2005) 'Enforced standards versus evolution by general acceptance: A comparative study of e□commerce privacy disclosure and practice in the United States and the United Kingdom', *Journal of accounting research,* 43(1), pp. 73-96.

Jamal, K., Maier, M. and Sunder, S. (2003) 'Privacy in E□Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market', *Journal of Accounting Research,* 41(2), pp. 285-309.

John, L. (2004) *Clueless office workers help spread computer viruses.* Available at: http://www.theregister.co.uk/2004/02/06/clueless_office_workers_help_spread/ (Accessed: 09/04/2015).

Johnson, R.B., Onwuegbuzie, A.J. and Turner, L.A. (2007) 'Toward a definition of mixed methods research', *Journal of mixed methods research,* 1(2), pp. 112-133.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M., Paxson, V. and Savage, S. (2008) *Spamalytics: An empirical analysis of spam marketing conversion.* ACM, pp. 3.

Khanna, S. and Chaudhry, H. (2012) *Anatomy of compromising email accounts.* IEEE, pp. 640.

Klien, S. (2004) *The privacy debate: this time it's personal.* Available at: http://www.theguardian.com/media/2004/apr/26/digitalmedia.mondaymediasection (Accessed: 29/07/2017).

Kortjan, N. and Von Solms, R. (2014) 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal,* 52, pp. 29-41.

Kritzinger, E. and Smith, E. (2008) 'Information security management: An information security retrieval and awareness model for industry', *Computers & Security,* 27(5), pp. 224-231.

Kritzinger, E. and von Solms, S.H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security,* 29(8), pp. 840-847.

Kumaraguru, P. and Sachdeva, N. (2014) 'Privacy4ICTD in India: Exploring Perceptions, Attitudes and Awareness about ICT Use', *arXiv preprint arXiv:1410.3942,* .

Kumaraguru, P. and Sachdeva, N. (2012) 'Privacy in India: Attitudes and awareness v 2.0', *Available at SSRN 2188749,* .

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F. and Hong, J. (2010) 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology (TOIT),* 10(2), pp. 7.

Kureva, G., Loock, M. and Kritzinger, E. (2014) 'Towards addressing Information Security Awareness through Internet Service Providers', .

Landesberg, M.K., Levin, T.M., Curtin, C.G. and Lev, O. (1998) 'Privacy online: A report to Congress', *NASA,* (19990008264).

Langendörfer, P., Maaser, M., Piotrowski, K. and Peter, S. (2008) 'Privacy-Enhancing Technique: A Survey and Classification' *Handbook of Research on Wireless Security* IGI Global, pp. 115-128.

Lawal, A. (2002) 'Entrepreneurship development in small and medium enterprises: key success factor', *Lagos Journal of Business,* 2(1), pp. 35-46.

Lee, D., Ahn, J. and Bang, Y. (2011) 'Managing consumer privacy concerns in personalization: a strategic analysis of privacy protection', *MIS Quarterly,* 35(2), pp. 423-444.

Leedy, P.D. and Ormrod, J.E. (2005) *Practical research*.

Legislation (2016) *Data Protection Act 1998.* Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/1 (Accessed:07/05/2015).

Lindlof, T.R. and Taylor, B.C. (2010) *Qualitative communication research methods.* Sage.

Lipka, M. (2013) *Avoid the perils of public Wi-Fi.* Available at: http://money.msn.com/saving-money-tips/post--avoid-the-perils-of-public-wi-fi. (Accessed:22/08/2014) .

MacDermott, S. and Smith, J. (2013) 'The Future of Privacy: A Consumer□Oriented Approach to Managing Personal Data Online', *Thunderbird International Business Review,* 55(1), pp. 3-12.

Madden, M., Rainie, L., Zickuhr, K., Duggan, M. and Smith, A. (2014) 'Public perceptions of privacy and security in the post-snowden era', *Pew Research Internet Project,* .

Markert, B. (2002) 'Comparison of three online privacy seal programs', *GSEC Practical Assignment Version,* 1.

Marotta-Wurgler, F. (2016) 'Understanding Privacy Policies: Content, Self-Regulation, and Markets', .

Marshall, C. and Rossman, G.B. (2014) *Designing qualitative research.* Sage publications.

Mathias, S. and Kazia, N. (2016) *Data protection in India: Overview.* Available at: http://uk.practicallaw.com/1-505-9607 (Accessed:16/03/2016) .

McCoy, C. and Fowler, R.T. (2004) *You are the key to security: establishing a successful security awareness program.* ACM, pp. 346.

McGettrick, A., Cassel, L.N., Dark, M., Hawthorne, E.K. and Impagliazzo, J. (2014) *Toward curricular guidelines for cybersecurity.* ACM, pp. 81.

Mcgroarty, P. and Hinshaw, D. (2014) *Nigeria's Economy surpasses South Africa in size.* Available at: http://www.wsj.com/articles/SB10001424052702304819004579485360572851126 (Accessed: 08/02/2015).

Mediati, N. (2011) *Secure Your Life in 12 Steps.* Available at: http://www.pcworld.com/article/225806/secure_your_life_in_12_steps.html (Accessed: 21/08/2016).

Meinert, D.B., Peterson, D.K., Criswell, J.R. and Crossland, M.D. (2006) 'Would regulation of web site privacy policy statements increase consumer trust?', *Informing Science,* 9, pp. 123.

Mellor, M. and Noyes, D. (2007) *Awareness and accountability in information security training.* Citeseer, .

Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, E.A. (1995) 'Values, personal information privacy, and regulatory approaches', *Communications of the ACM,* 38(12), pp. 65-74.

Milberg, S.J., Smith, H.J. and Burke, S.J. (2000) 'Information privacy: Corporate management and national regulation', *Organization science,* 11(1), pp. 35-57.

Miles, M.B., Huberman, A.M. and Saldana, J. (2013) *Qualitative data analysis.* Sage.

Miltgen, C.L. and Smith, H.J. (2015) 'Exploring information privacy regulation, risks, trust, and behaviour', *Information & Management,* 52(6), pp. 741-759.

Ministry of Law, Justice and Company Affairs (2000) 'The Information Technology act', .

Miyazaki, A.D. (2008) 'Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage', *Journal of Public Policy & Marketing,* 27(1), pp. 19-33.

Morse, J.M., Barrett, M., Mayan, M., Olson, K. and Spiers, J. (2002) 'Verification strategies for establishing reliability and validity in qualitative research', *International journal of qualitative methods,* 1(2), pp. 13-22.

Muhammad, H. (2015) *CBN warns against scammers as BVN registration ends today* . Available at: http://www.dailytrust.com.ng/news/general/cbn-warns-against-scammers-as-bvn-registration-ends-today/117236.html (Accessed: 21/03/2017).

Myers, M.D. (1997) 'Qualitative research in information systems', *Management Information Systems Quarterly,* 21(2), pp. 241-242.

National Information Technology Development Agency (2013) *Guidelines on Data Protection Draft.* Available at: http://www.nitda.gov.ng/download/dataprotection.pdf (Accessed: 15/02/2016).

National Initiative for Cybersecurity Education (2015) *The National Initiative for Cybersecurity Education (NICE).* Available at: http://csrc.nist.gov/nice/awareness.html (Accessed: 20/08/2015).

NCSA (2015) *Stay Safe online.* Available at: http://staysafeonline.org/ (Accessed:12/05/2016) .

Ncube, C. (2004) 'A comparative analysis of Zimbabwean and South African data protection systems', *Journal of Information, Law & Technology,* (2), pp. 18.

ngCert (2014) *ngCert, About.* Available at: https://www.cert.gov.ng/about (Accessed:08/02/2015).

Niranjanamurthy, M. and Chahar, D.D. (2013) 'The study of e-commerce security issues and solutions', *International Journal of Advanced Research in Computer and Communication Engineering,* 2(7).

Niranjanamurthy, M., Kavyashree, N., Jagannath, S. and Chahar, D. (2013) 'Analysis of e-commerce and m-commerce: advantages, limitations and security issues', *International Journal of Advanced Research in Computer and Communication Engineering,* 2(6).

Nonaka, I. and Takeuchi, H. (1995) *The knowledge-creating company: How Japanese companies create the dynamics of innovation.* Oxford university press.

Oates, B.J. (2005) *Researching information systems and computing.* Sage.

Obutte, P.C. (2014) 'ICT laws in Nigeria: planning and regulating a societal journey into the future', *PER: Potchefstroomse Elektroniese Regsblad,* 17(1), pp. 01-35.

OECD (2013) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD.* Available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Accessed: 10/13/2015).

Oludare, R. (2015) *CSEAN kicks off cyber security awareness campaign, expansion | The Guardian Nigeria.* Available at: http://www.ngrguardiannews.com/2015/07/csean-kicks-off-cyber-security-awareness-campaign-expansion/ (Accessed: 8/24/2015).

Orlikowski, W.J. and Baroudi, J.J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information systems research,* 2(1), pp. 1-28.

Oyelami, O., Okuboyejo, S. and Ebiye, V. (2013) 'Awareness and usage of Internet-based health information for self-care in Lagos State, Nigeria: implications for healthcare improvement', *Journal of Health Informatics in Developing Countries,* 7(2), pp. 165-177.

Park, Y.J. (2013) 'Digital literacy and privacy behavior online', *Communication Research,* 40(2), pp. 215-236.

Parr, B. (2014) *20,000+ Gmail, Yahoo, AOL Accounts Compromised [ALERT].* Available at: http://mashable.com/2009/10/06/gmail-accounts-exposed/ (Accessed: 08/24/2015) .

Pathirage, C., Amaratunga, D. and Haigh, R. (2008) 'The role of philosophical context in the development of theory: Towards methodological pluralism', *The Built and Human Environment Review,* 1(1).

Penenberg, A. (2005) *Cookie Monsters: The innocous text files that web surfers love to hate.* Available at: http://www.slate.com/articles/technology/technology/2005/11/cookie_monsters.html. (Accessed: 13/02/2015).

Perchstone & Graeys (2016) *Data Protection in Nigeria: A call for a single legislative framework.* Available at: http://www.mondaq.com/Nigeria/x/531396/data+protection/Data+Protection+In+Nigeria+A+Call+For+A+Single+Legislative+Framework (Accessed: 11/03/2017).

Provos, N., McNamee, D., Mavrommatis, P., Wang, K. and Modadugu, N. (2007) *The ghost in the browser analysis of web-based malware.* pp. 4.

Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S. and Furnell, S. (2015) 'A systematic review of approaches to assessing cybersecurity awareness', *Kybernetes,* 44(4), pp. 606-622.

Ramzan, Z. (2010) 'Phishing attacks and countermeasures' *Handbook of Information and Communication Security* Springer, pp. 433-448.

Reid, R. and Van Niekerk, J. (2014) *Towards an Education Campaign for Fostering a Societal, Cyber Security Culture.* pp. 174.

Roth, W.D. and Mehta, J.D. (2002) 'The Rashomon effect: Combining positivist and interpretivist approaches in the analysis of contested events', *Sociological Methods & Research,* 31(2), pp. 131-173.

Rouse, M. (2014) *Personally identifiable information (PII).* Available at: http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information (Accessed: 05/09/2016) .

Rouse, M. (2008) *HTTPS (HTTP over SSL or HTTP Secure).* Available at: http://searchsoftwarequality.techtarget.com/definition/HTTPS (Accessed: 24/08/2015).

Rudraswamy, V. and Vance, D.A. (2001) 'Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment', *Logistics Information Management,* 14(1/2), pp. 127-137.

Sampson, P. (2013) 'Data Protection Act: Privacy & Security in the Information Age', .

SANS (2014) *Securing the Human.* Available at: https://securingthehuman.sans.org/ (Accessed: 08/02/2015).

Sarantakos, S. (2005) 'Social Research. 3rd', *Hampshire: Palgrave Macmillan,* .

Sarathy, R. and Robertson, C.J. (2003a) 'Strategic and ethical considerations in managing digital privacy', *Journal of Business Ethics,* 46(2), pp. 111-126.

Sarathy, R. and Robertson, C.J. (2003b) 'Strategic and ethical considerations in managing digital privacy', *Journal of Business Ethics,* 46(2), pp. 111-126.

Saunders, M.L. and Lewis, P. (2009) 'P. & Thornhill, A.(2009)', *Research methods for business students,*.

Seckler, M., Heinz, S., Forde, S., Tuch, A.N. and Opwis, K. (2015) 'Trust and distrust on the web: User experiences and website characteristics', *Computers in Human Behavior,* 45, pp. 39-50.

Sekaran, U. and Bougie, R.J. (2016) *Research methods for business: A skill building approach.* John Wiley & Sons.

Seničar, V., Jerman-Blažič, B. and Klobučar, T. (2003) 'Privacy-enhancing technologies—approaches and development', *Computer Standards & Interfaces,* 25(2), pp. 147-158.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H. (2009) 'The impact of information richness on information security awareness training effectiveness', *Computers & Education,* 52(1), pp. 92-100.

Siponen, M.T. (2000) 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security,* 8(1), pp. 31-41.

Skinner, G., Han, S. and Chang, E. (2006) 'An information privacy taxonomy for collaborative environments', *Information management & computer security,* 14(4), pp. 382-394.

Smith, H.J., Dinev, T. and Xu, H. (2011) 'Information privacy research: an interdisciplinary review', *MIS quarterly,* 35(4), pp. 989-1016.

Stake, R.E. (1995) *The art of case study research.* Sage.

Steinke, G. (2002) 'Data privacy approaches from US and EU perspectives', *Telematics and Informatics,* 19(2), pp. 193-200.

Stopthinkconnect (2014) *Keeping the web a safer place for everyone.* Available at: https://www.stopthinkconnect.org/ (Accessed: 08/02/2015).

Suleiman, M., Mohammed, D., Abdullahi Aliyu, D. and Muhammad, A. (2015) 'Enhanced approach for cyber security web applications in Nigeria', .

Sundstrom, E., Burt, R.E. and Kamp, D. (1980) 'Privacy at work: Architectural correlates of job satisfaction and job performance', *Academy of Management Journal,* 23(1), pp. 101-117.

Symantec Norton (2012) 'Norton Cybercrime Report," 2012', .

Taddicken, M. (2014) 'The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self□disclosure', *Journal of Computer□Mediated Communication,* 19(2), pp. 248-273.

Tajpour, A., Ibrahim, S. and Zamani, M. (2013) 'E-Commerce and Identity Theft Issues', *International Journal of Advancements in Computing Technology,* 5(14), pp. 105.

Talib, S., Clarke, N.L. and Furnell, S.M. (2010) *An analysis of information security awareness within home and work environments.* IEEE, pp. 196.

Tayo, O., Thompson, R. and Thompson, E. (2016) 'Impact of the Digital Divide on Computer Use and Internet Access on the Poor in Nigeria.' *Journal of Education and Learning,* 5(1), pp. 1-6.

The Economist (2014) *Africa's New Number One.* Available at: http://www.economist.com/news/leaders/21600685-nigerias-suddenly-supersized-economy-indeed-wonder-so-are-its-still-huge (Accessed: 24/08/2016).

Thompson, H. (2008) *How I Stole Someone's Identity.* Available at: http://www.scientificamerican.com/article/anatomy-of-a-social-hack/ (Accessed: 05/09/2016)

Transparency International (2015) *Nigeria.* Available at: http://www.transparency.org/gcb2013/country/?country=nigeria (Accessed: 11/02/2016).

TRUSTe (2017a) *TRUSTe.* Available at: http://www.truste.com/about-TRUSTe/ (Accessed: 07/03/2017)

TRUSTe (2017b) *TRUSTe Program Requirements.* Available at: http://www.truste.com/privacy-program-requirements/program- requirements (Accessed: 07/03/2017)

TRUSTe (2013) *Truste Transparency Report (abstract)*.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008) 'Investigating information security awareness: research and practice gaps', *Information Security Journal: A Global Perspective,* 17(5-6), pp. 207-227.

UK Government Cabinet Office (2013) *Protecting and promoting the UK in a digital world: 2 years on.* Available at: https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world-2-years-on (Accessed: 02/08/2015).

Uma, K. and Eboh, F. (2013) 'Corruption, economic development and emerging markets: evidence from Nigeria', *Asian Journal of Maanagement Sciences and Education,* 2(3).

Vconnect (2017) *Vconnect.* Available at: https://business.vconnect.com/ (Accessed:09/04/2017).

Veghes, C., Pantea, C., Balan, D. and Lalu, B. (2009) 'European Union consumers 'views on the protection of their personal data: an exploratory assessment', *Annales Universitatis Apulensis: Series Oeconomica,* 11(2), pp. 988.

Venkatesh, V., Brown, S.A. and Bala, H. (2013) 'Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems.', *MIS quarterly,* 37(1).

Veseli, I. (2011) 'Measuring the Effectiveness of Information Security Awareness Program', .

Wahyuni, D. (2012) 'The research design maze: Understanding paradigms, cases, methods and methodologies', .

Wang, P., Hawk, W.B. and Tenopir, C. (2000) 'Users' interaction with World Wide Web resources: An exploratory study using a holistic approach', *Information processing & management,* 36(2), pp. 229-251.

Warren, S.D. and Brandeis, L.D. (1890) 'The right to privacy', *Harvard law review,* , pp. 193-220.

Wilson, M. and Hash, J. (2003a) 'Building an information technology security awareness and training program', *NIST Special publication,* 800, pp. 50.

Wilson, M. and Hash, J. (2003b) 'Building an information technology security awareness and training program', *NIST Special publication,* 800, pp. 50.

Wired Safety (2014) *The world'd first Internet Safety and help group.* Available at: https://www.wiredsafety.org/ (Accessed: 08/02/2015).

Wolf Park and Digital Jewels (2014) *The Nigerian Cyber threat barometer report.* Available at https://www.wolfpackrisk.com/assets/docs/NIgerianCyberThreatBarometer_2014(Med_Res).pdf:(Accessed:19/08/2015).

Woon, I., Tan, G. and Low, R. (2005) 'A protection motivation theory approach to home wireless security', *ICIS 2005 Proceedings,* , pp. 31.

Yin, R.K. (2013) *Case study research: Design and methods.* Sage publications.