Mitigation of data breaches for online customers in South Africa

Michael Saunders Shepperson

9809905P

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

Johannesburg, 2018

Protocol number: WBS/ba9809905P/710

DECLARATION

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

Michael Saunders Shepperson

Signed at ……

On the …….. day of …… 20…..

DEDICATION

This Research Article is dedicated to my parents Joan and Tony Shepperson and to my sister Gillian. Thank you for all the love and support you have given me during this time. This has been a mammoth year, with a lot of ups and downs. Despite these ups and downs you were the constant I could rely upon.

Thank you so much.

ACKNOWLEDGEMENTS

I would like to acknowledge a number of people for the support and guidance that they gave me while I was completing my MBA.

Firstly, to my supervisor Sam Kula, thank you so much for the time and guidance you gave me in getting this research done

Secondly, to the academic staff of Wits Business School, in particular, Professor Anthony Stacey, for the research boot camps, you organised. Without them, I would have been lost. To Charisse Drobis, thank you for always being there to listen to my complaints, and offering me advice. A special thanks to Mike Mundy, for all the practical advice you gave me.

Thirdly, to my fellow MBAs, Pierre thanks for always being there to listen to my complaints and letting me run things by you. To Rishal, thanks for all the technical advice you gave me and the extra lessons. To Terri, thanks for always being there to vent to. To Cradle, my first syndicate group, thank you for a wonderful experience, you guys set the tone for the MBA.

Finally, to my Sunshine in the North, Amina. Thank you so much for all the support you gave me while doing this MBA. You were always the constant that I could rely upon. Even though you live so far away, you were still there for me. أنت دائما في قلبي

SUPPLEMENTARY INFORMATION

Nominated journal:	Journal of Contemporary Management
Supervisor / Co-author:	Mr Sam Kula
Word count †:	12,861
Supplementary files:	Questionnaire

† Including abstract references, etc.

ABSTRACT

Technological advances and increasing access to the internet has allowed customers from all over the world to access online shopping platforms. This has contributed significantly to the growth of the customer base of online shopping companies. Cybercrime has emerged as the biggest threat to the online shopping industry. All online shopping companies face the risk of a cyber-attack, generally through a data breach. These data breaches compromise the personal and financial details of the customer base, exposing customers to a further broad range of cybercrimes. Many online shopping companies believe they will not be exposed to a data breach and rely heavily on outdated cybersecurity infrastructure and procedures. Furthermore, these companies do not have a comprehensive Data Breach Response Plan to utilise in the event of a data breach. However, in the event of a data breach, many companies just do not know how to retain their customer base. Data collected quantitatively from respondents who shop online, via an electronic survey, examines what methods and attributes an online shopping company could use or offer to its affected customer base to retain their patronage. Data breaches negatively impact the trust a customer has in the online shopping company. It is this trust initially that convinces a customer to utilise the services of the online shopping company. Online shopping companies need to offer a wide range of attributes to retain some of their customer base. However, despite providing customers with every conceivable option, there is a strong possibility that an online shopping company will only be able to retain roughly half the customers that were affected by the data breach. Online shopping companies need to establish and maintain a comprehensive cybersecurity policy and ensure that their staff are fully trained. Overall, online shopping companies need to develop more comprehensive cybersecurity policies to help militate against the threat of data breaches, as a data breach can efficiently extinguish customer trust, which online shopping companies need to conduct business.

Keywords: Online Shopping, Data Breaches, Retaining Customers, Cybercrime, Customer Trust

1. Introduction

As technology has advanced and with the aid of the internet, online shopping has grown exponentially worldwide, giving customers from around the world access to online shopping platforms (Panda & Swar, 2013). However, with this growth, the threat of cybercrime has also increased, threatening online shopping companies through data breaches. These breaches can potentially affect the personal and financial data of customers who utilise online shopping platforms. Despite every precaution taken by an online shopping company, there is still a risk that they will be affected by a data breach (Disparte & Furlow, 2017). Online shopping companies need to develop methods on how to restore the confidence of their customer base in the event of a data breach.

Purpose of the study

The purpose of this study is to determine how online shopping companies can attempt to restore the trust of their customer base following a data breach.

Context of the study

Online shopping was first introduced in 1979 by English inventor Michael Aldrich (Geetha & Rangarajan, 2015). Since then rapid technological advances and the internet have created a new environment for companies to conduct business digitally. These digital advances have improved the efficiency and convenience of doing business, making it more attractive (Mallapragada, Chandukala, & Liu, 2016). This has given rise to the concept of online shopping, an alternative to traditional shopping, by allowing consumers to shop in the comfort of their own home (Mallapragada et al., 2016). Additionally, technology has advanced to the point whereby consumers can shop online for consumer goods via a smartphone further penetrating the market (Panda & Swar, 2013).

Numerous companies have branched out into the e-commerce sector, creating an online platform that advertises a variety of goods and products to their customers (Mallapragada et al. 2016). In some cases, companies offer products not readily available in some countries (Mallapragada et al. 2016). In order to make their services even more attractive some companies offer free delivery of the product as an added incentive, the economic spending data from customer's

browsing history and purchasing history is used by online shopping companies to help create a marketing profile of a customer and used to advertise products to cater for these needs and interests (Mallapragada et al. 2016). As payment of products is made electronically, online companies have created accounts for customers to store their financial details on the profile for convenience. Some companies handle the electronic payments themselves, while other companies utilise a third party to facilitate electronic payments, such as PayPal (Mintzer, 2014). It is often inconvenience cited as the main reasons why customers will break their relationship with a company (Moeller, Fassnacht, & Ettinger, 2009).

However, the use of the internet has also created a new threat, cybercrime. Many businesses and individuals are usually unaware of the potential risk they face and are often unprepared when faced with a cybersecurity breach or more commonly known as a cyber-attack. Cybercrime is defined as any crime that utilises an electronic device such as a laptop, computer and cell phone and takes place within the electronic environment (Spalević, 2014).

Many companies do not take this threat seriously and play down the risk it poses (Banham, 2017). It is crucial for companies to understand the dangers of cybercrime and accept the reality of when it happens and not if it will happen (Banham, 2017). All businesses are susceptible to cyber-attacks, including small businesses. Alexander (2015) states that in this day and age, the majority of small businesses utilise the internet to create business and run the day to day operations. Several owners of small businesses believe they are too insignificant to be threatened by cyber-attacks. However, Banham (2017) argues small businesses present a natural opportunity for hackers to steal financial data from customers. Even the most sophisticated cyber security systems face constant vulnerabilities. Thus, continuous assessment of a business's cybersecurity measures is needed (Banham, 2017).

Numerous companies rely on standard forms of cyber security, while other companies do not place much emphasis on it (Cheng & Groysberg, 2017). According to Hewes Jr. (2016) companies need to have a standard cybersecurity policy in place that covers all potential threats; secondly, companies need to have

a comprehensive training program in place for new employees, and finally, the technology used by the company needs to be secure. Similarly, Disparte and Furlow (2017) argue that most companies do not invest much in cybersecurity training and programmes for new employees. Human error is the primary cause of cyber security breaches within most companies (Disparte & Furlow, 2017). Most companies only evaluate their cybersecurity policy after a breach has occurred (Cheng & Groysberg, 2017).

This can be attributed to the way managers make decisions. Many managers fall into a mindset and a habitual way of conducting business, and only react after a data breach has occurred (Grant, 1988). This dominant management logic hinders management's ability to inversely respond to a threat (Grant, 1988). With the number of breaches increasing each year, companies will have to mitigate the danger by ensuring their cybersecurity systems are up to date (Disparte & Furlow, 2017). And in the event of a cyber breach, online shopping companies need to develop a strategy to respond to the impact of the breach and mitigate the fears and concerns of their customer base to keep them utilising their services and convince them not to move away to other competitive online shopping companies. Furthermore, retaining customer loyalty after a data breach is the most significant challenge facing companies. As many companies do not take cybersecurity threats seriously, many more do not even have a data breach response plan to use in the event of a data breach.

Importance and Relevance of the Research

Online shopping is increasing steadily and becoming a more common method for a number of customers to shop. This is mainly due to the convenience it offers. Cybercrime is also growing, and the number of data breaches that have affected companies is steadily increasing annually. Companies that operate in cyberspace will at one time in their existence suffer from a data breach, and the majority of managers and leaders of these companies often make several common mistakes, which inadvertently adds to the crisis (Bourdon, 2017). Managers and leaders are often slow to respond to data breaches and have a tendency to try and hide this information from customers (Bourdon, 2017). There is a need to understand what methods an online shopping company can utilise after a data

breach has occurred in order to help alleviate any fears existing customers have, and thus prevent customers from moving to other online shopping companies. Additionally, a large number of these online shopping companies have created a brand. Data breaches can easily harm a company's brand as well as the relationship of trust between the customer and company (Whitler & Farris, 2017).

Delimitations of the Study

The study will examine how customers respond to data breaches, and how companies in turn attempt to restore the confidence of their customer base using various methods. The study will not include any in-depth technical analysis of cyber security and prevention of data breaches. For the purpose of this study, online shopping will refer to the exchange of money electronically for consumer goods and not services.

2. Literature Review

The creation of cyberspace has created the information age, whereby vast amounts of information flow freely around the world via the internet. Between 1999 and 2000, the commercial use of cyberspace was established and allowed all people from around the globe to connect and communicate with each other (Barik, Soni, & Pandey, 2015). As technology has advanced in the past few decades, individuals, companies and governments have become more reliant on the internet and electronic devices that give them access to the internet (Gupta, 2014). The internet has allowed companies to enter the global market where anyone in the world is a potential customer. This in effect has opened up a new market that has no borders or boundaries. However, the internet has opened up a new avenue of criminal activity. Cybercrime is defined as illegal activities carried out by means of computers or the internet (Dennis, 2017). As technology has progressed, cellular phones are able to access the internet, and as such can potentially be used to carry out a cybercrime (Buck, 2012).

What is Cyber Security and what threats do online businesses face?

According to Lord (2017) cybersecurity or information technology security refers to the technological practices and processes created for the purpose of protecting computer networks and the information stored and shared on these networks.

According to Daniel (2017) cybersecurity is a concept that does not remain within the technical realm. Cybersecurity encompasses a broader outlook and does not follow the rules of everyday life. For example, everyone is responsible for their own protection in the cyber world. Individuals, governments and businesses take it upon themselves to protect themselves from any form of attack in the cyber world. In the real world, individuals and companies would rely on law enforcement agencies to provide that security (Daniel, 2017). Also, policing cybercrime is still very much in its infancy. Governments from around the world have various policies in place to police cyberspace, making it very difficult to combat cybercrime universally (Daniel, 2017). Additionally, cyber threats are evolving continuously, making it very difficult for cybersecurity frameworks (Lord, 2017).

According to IBM chairperson Ginni Rommerty, cybercrime is the most significant threat to every company in the world (Morgan, 2017). Cybercrimes worldwide cost the global economy over $3 trillion in 2016 and costs are expected to rise to $6 trillion by 2021 annually (Morgan, 2017). According to Gyunka and Christiana (2017), most common cybersecurity vulnerabilities are caused by human error. The vulnerabilities posed by human error constitute careless work practices, disregard of cybersecurity policies and the negligent storage of sensitive materials, both physically and electronically (Gyunka & Christiana, 2017). These vulnerabilities can easily be exploited by an internal or external threat, namely a hacker. Social engineering is the most common method used by cybercriminals to obtain sensitive information from people. Typical social engineering tactics include phishing scams, malware attacks and engaging with people in fake voice calls (Gyunka & Christiana, 2017).

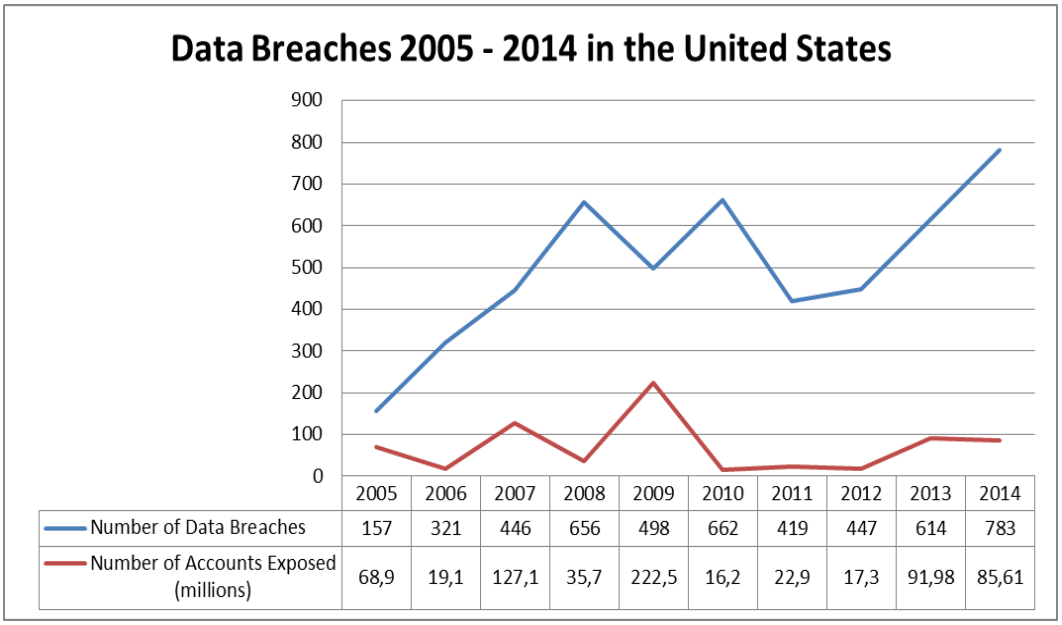
According to Hewes Jnr, (2016) companies that are victims of cyber-attacks often suffer from numerous effects such as

1) The potential loss and theft of company funds
2) The possible interruption of critical operations of the company
3) Damage to the network infrastructure of the business and equipment
4) The theft or loss of confidential information of customers
5) Damage to a company's business reputation (Hewes Jr., 2016).

Cybercrime, described as any criminal activity conducted electronically by Julisch (2013), have become increasingly common. Additionally, these threats have become more frequent, sophisticated and are now becoming targeted which poses a severe threat, not only to governments but also to businesses and their customers (Choo, 2011). Customers are often affected by data breaches and fall prey to a number of cybercrimes. Usually, the financial details of a customer are customarily compromised after a breach, leading to compromised credit card details, which hackers use to make illegal purchases. Additionally, identity theft is another crime that affects customers (IT News Africa, 2017).

Data breaches are increasing steadily on an annual basis. In the first half of 2017, there were 918 data breaches recorded worldwide that compromised over 1.9 billion data records (Foltyn, 2017) In 2016, 4,129 data breaches occurred worldwide, resulting in over 4.2 billion accounts being compromised. Roughly 53% of these breaches were the result of hackers (Roberts, 2017). In 2015, 1,673 data breaches occurred worldwide compromising over 707 million accounts (Security Week News, 2016).

According to Lord (2017), the number of data breaches in the United States steadily increased from 2005 to 2014. The United States remains the leading country that experiences the most data breaches (Foltyn, 2017).



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Number of Data Breaches	157	321	446	656	498	662	419	447	614	783
Number of Accounts Exposed (millions)	68,9	19,1	127,1	35,7	222,5	16,2	22,9	17,3	91,98	85,61

Figure 1 Number of Data Breaches and Exposed Accounts 2005 – 2014 in the United States (Lord, 2017)

According to the United States Department of Justice, cyber-attacks increased from 1,000 attacks a day in 2015 to over 4,000 attacks a day in 2016, a significant increase (Banham, 2017). Similarly, in the United Kingdom (UK), cyber breaches involving the loss of customer's personal information including their financial data increased from 19 incidents in 2015/16 to 38 incidents in 2016/17 (The Telegraph, 2017).

Numerous examples of data breaches exist. In 2013, United States retail store Target suffered a data breach resulting in the credit card details of 41 million customers being compromised. On May 23, 2017, Target paid reparations of $18.5 million to customers that were affected by the breach. Hackers obtained access to Target's customer database after stealing credentials from a third-party vendor. After installing malware software, hackers obtained full names, credit card details and other personal information of customers and exploited this information (McCoy, 2017)

The most prominent threat to cybersecurity often comes from inside an organisation, through simple human error (Vest, 2017). According to IBM, 95% of all cyber security incidents within companies are the result of human error. As Zandelhoff (2016) argues human error constitutes a wide range of attributes, such as employees visiting unauthorised websites, clicking on suspicious links in

emails, falling prey to phishing scams and general tardiness towards cybersecurity policy.

The Concept of Online Shopping

According to (Girish, Chandukala, & Liu, 2016) online shopping provides an alternative to traditional shopping. The ease and convenience of online shopping give a much better alternative to standing in lines and dealing with the hassle of going out to shop.

Technological advances have allowed customers to shop from laptops, smartphones devices and tablets (Statista: The Statistics Portal, 2016). However, from the table below, Laptops and Personal Computers still remain the most prominent methods for online shopping.

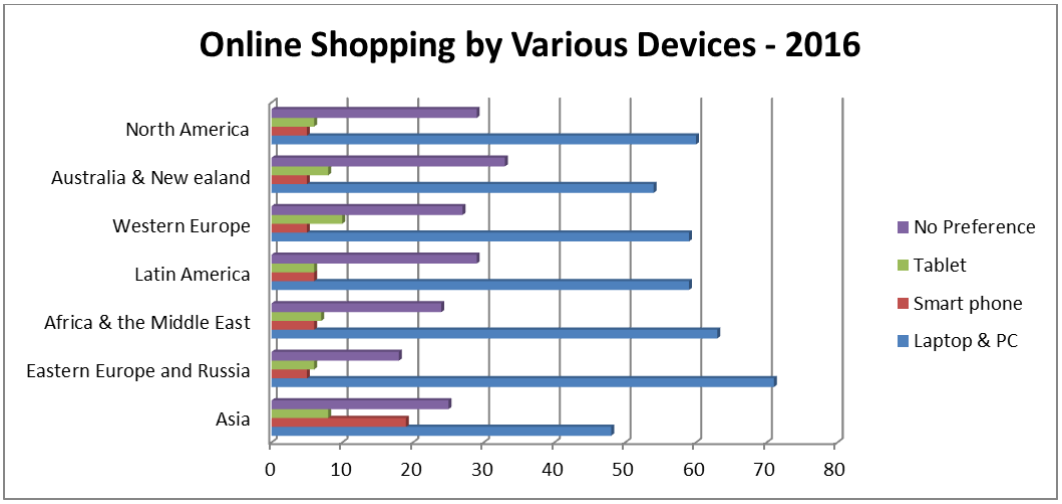


Figure 2 Online Shopping Figures by Various Devices 2016 (Statista: The Statistics Portal, 2016)

According to Figure 3, e-commerce sales worldwide have increased significantly since 2014, generating $1, 336 billion in 2014 and are expected proliferate over the next four years. In 2021, worldwide e-commerce sales are expected to reach $4,479 billion in revenue. In 2016, it was estimated that roughly 1.6 billion people shopped online globally, this includes shopping for goods and services. In South Africa, online shopping constitutes approximately 1% of total retail sales in the country; this equates to roughly R1 billion in online sales and is expected to grow significantly within the following years (Mahlaka, 2016)

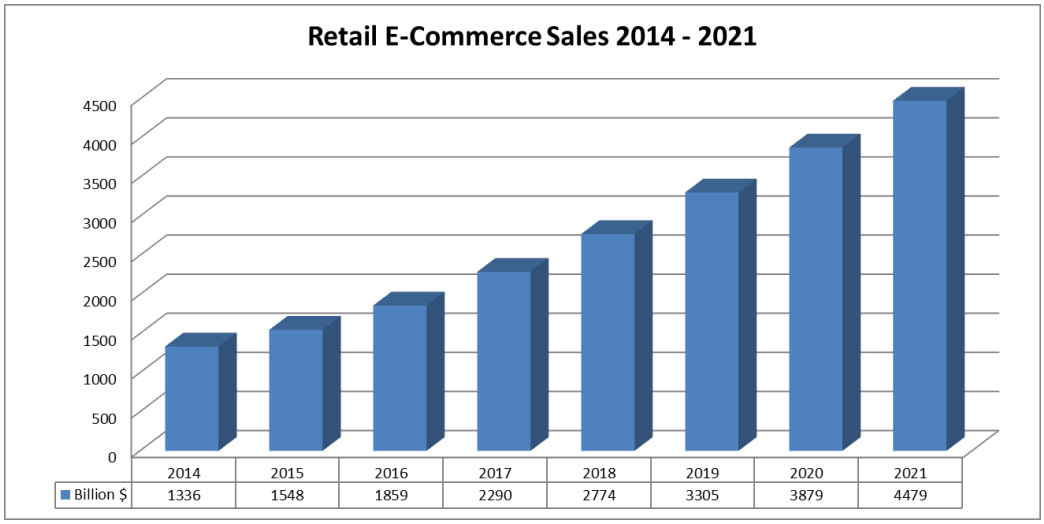


Figure 3 Depicts Worldwide E-commerce Retail Sales 2014 – 2021 (Statista The Statistics Portal, 2017)

Customers who use online shopping place a lot of trust in the services of the companies that they buy products from. In order to maintain this level of trust companies need to be reliable, trustworthy and keep a good reputation in order for this level of trust to continue (Bernard & Makienko, 2011). However, despite the growth in online shopping, a large number of customers still perceive online shopping a significant degree of risk (Hsieha & Tsao, 2014). Hsieha and Tsao (2014) identify three significant concerns from customers. Firstly, the customer may never receive the product they ordered, secondly, they may accidentally purchase the incorrect product and lastly; their financial and personal information may be compromised.

Dealing with Data Breaches; Maintaining a Company's Reputation

It is not a matter of if but a matter of when companies, organisations and individuals will be victims of some sort of cyber-attack (Vinton, 2014). In the event of a data breach, companies are faced with numerous challenges. For starters, the reputation and share price of a company that is usually breached is negatively affected (Bischoff, 2017). Data breaches can harm the reputation of a company to a certain degree, but how a company responds to the data breach can affect the reputation considerably (Drinkwater, 2016). However, according to Rikallah (2017), the stigma attached to a company that has suffered a breach is not as severe as it used to be. The stigma is now based on how a company responds to the data breach (Rizkallah, 2017). Additionally, the trust a customer has in a

particular company is severely damaged and the brand a company has spent so much time building up can easily be damaged beyond repair (Whitler & Farris, 2017).

Proper cyber awareness training is instrumental in helping online shopping companies militate against future cyber-attacks (Disparte & Furlow, 2017). As human error contributes to the majority of attacks, a proper cybersecurity culture needs to be implemented and maintained. The maintenance of a cybersecurity awareness culture is instrumental in how companies are able to deal with a possible data breach. Additionally, the leadership of companies need to understand that any cybersecurity policy in place needs to be regularly updated and become a strategic priority.

Despite these cyber-attacks, roughly a third of UK companies, surveyed by the UK government had not spent any additional money to improve their cybersecurity measures (The Telegraph, 2017). According to internet security company Norton, roughly 9 million South Africans were victims of cybercrime in 2015 (Zyl, 2016). According to Graham Croock, director of IT Audit, Risk and Cyber Lab at BDO, a large number of South African business are entirely unprepared for cyber-attacks and are relying on out-dated strategies and technology (Alfreds, 2016)

One of the major problems arising is convincing businesses leaders and the management of companies of the seriousness of this threat. Far too many businesses tend to focus on other priorities. It is estimated that a data breach in a large corporation can cost a corporation roughly $4 million. Additionally, according to Cheng and Groysberg (2017) management often lack the expertise when attempting to decide on how to deal with the issue of cybersecurity. As Disparte and Furlow (2017) argue, companies need to break from the traditional approach to dealing with cyber threats, by believing that current technological systems in place will deal with the problem.

Formulating a Data Breach Response Plan

Despite every precaution taken, data breaches do occur, and online shopping companies need to protect the interests of the customer in order to continue doing business. By not acting quickly, decisively, honestly and taking full responsibility customer trust will be damaged (Hilburg, 2013). As Hilburg (2013) states most companies only have a template of a data breach response plan. This template allows companies to develop and customise the response plan quickly. With the internet, customer dissatisfaction can spread rapidly and contribute negatively to a companies' reputation, through the use of social media (Shiue & Li, 2013). Ultimately a data response team is formulated to protect the customers and to protect the brand name of the company (Lewis, 2002). However, as Lord (2017) suggests, a cross-functional team is needed to respond to a data breach. A number of attributes or methods can be used to help restore a customer's willingness to utilise the services of the affected online shopping company.

A Clear, Concise Communications Policy Needed

Firstly, as Kohgadai (2016) states an efficient communications team is needed. No company wishes to admit that their system has been breached as it immediately creates panic amongst customers, but it is essential to inform your customer base of what the problem is. It is also essential for management to understand that customers react to these breaches emotionally, and when management fails to recognise this issue, customers will become irate and will start to look for alternative options (Tybout & Roehm, 2009). Therefore, it is imperative to formulate a strategic response to the incident. The communications team needs to apologise to the customers, who are affected and those not affected. The message created must be managed by the crisis response team and only this team. Conflicting messages can often cause more harm than good. Communication internally and externally must come from one source (Bende & Barnard, 2006).

Furthermore, messages conveyed by the response team to the customer base need to address the severity of the breach and explain the effect it has on customers. These messages must be legible, concise and not heavily laden with jargon (Bende & Barnard, 2006). The communications team must also be responsible for cooperating with various law enforcement agencies and

communicating with them regularly (Goldberg, 2013). The communications team can also put customers in touch with law enforcement agencies, in the event their personal and financial data were compromised.

Technical Support

Secondly, a technical response team is needed to assess the damage of the breach and determine how many customers were affected and what sort of information was compromised. More importantly, a technical response team needs to learn how the breach occurred and how to prevent a breach from happening again (Lord, 2017). Another important aspect the technical response team needs to do is to educate its staff on how the breach occurred and how to prevent it from happening again (Lord, 2017). The technical response team can help customers reset their personal passwords, in order to ensure their accounts cannot be compromised further. Furthermore, these teams can provide first-hand expertise and handle any technical queries from customers affected by the breach and customers concerned about the breach who have not been affected (Ragan, 2016).

Customer Relations Management

Thirdly, a customer relations management team needs to be established to mitigate the effect of the breach on the customer base. Customers become emotional when there is a possibility that personal and financial information has been compromised. According to Choi, Kim and Jiang (2016), customer's perspectives and behaviours towards a company will depend on how a company responds to a crisis (Choi, Kim, & Jiang, 2016). Thus, the establishment of a customer management team, dedicated to deal with customers' concerns and issues is necessary to maintain a customer base. Furthermore, as Choi et al., (2016), argue, good quality service will influence a customer's willingness to recommend the services of a company.

Compensation is usually an excellent method used by companies to retain their customer base. However, it is unfortunately costly, as some companies may not be in a financial position to accommodate financial compensation or even a full refund (Goode, Hoehle, Venkatesh, & Brown, 2017). However, compensation

expectations differ between customers depending on the severity of the breach and as such is very difficult to gauge the level of compensation needed to satisfy all customers affected (Goode et al., 2017). This can lead to dissatisfaction amongst customers if too little compensation is offered and has to be handled very carefully.

In the event of a data breach, online shopping companies need to address the issue of an apology, technical assistance, legal assistance, compensation and finally the effect of a full refund.

3. Problem Statement and Research Objectives

Main Problem

The purpose of this study is to ascertain what attributes and or methods an online shopping company can utilise to retain their customer base after a data breach.

Sub Problem

The subproblem seeks to gauge the impact of these methods or attributes, individually or in combination, on the customer base that has been affected by a data breach. The data was collected via electronic surveys from a comprehensive range sample and was tested through a quantitative approach.

Propositions

The objectives of this research are to determine which attributes or combination of attributes will have the most significant positive impact on customers who have been affected by a data breach:

1) Proposition 1 – No response from an online shopping will have a positive effect on customers who are affected by a data breach
2) Proposition 2 - An apology on its own will have a positive impact on customers who are affected by a data breach
3) Proposition 3 – An apology and free legal assistance will have a positive impact on customers affected by a data breach
4) Proposition 4 – An apology, free technical and legal assistance will have a positive impact on customers affected by a data breach

5) Proposition 5 – An apology, free technical and legal assistance and some compensation will have a positive impact on customers affected by a data breach
6) Proposition 6 – An apology, free technical assistance and full compensation will have a positive impact on customers affected by a data breach
7) Proposition 7 – An apology, free technical and legal assistance and a full refund will have a positive impact on customers affected by a data breach

Hypothesis

Following a data breach in which the financial and personal data of customers has been compromised, online shopping companies will be able to retain their customer base.

4. Research Methodology

The primary aim of this research report is to determine how online shopping companies can rebuild customer trust and confidence and retain their current customers, following a data breach. This section will outline the methodology selected in order to determine what methods an online shopping company can use in order to help retain their customer base, those affected and those not affected. Furthermore, this section will outline the questionnaire design, the population sample, the collection of the data and the method of analysis used to interpret the data collected.

A quantitative approach will be taken when conducting research for this research report. According to Creswell (2003), quantitative research is the method in which a researcher will use post-positivist claims for developing results through the use of measurement by collecting data that yields statistical results. Electronic surveys will be employed to obtain data from respondents who shop online. The purpose of a survey is to measure variables, such as attitudes, behaviours and traits amongst a population in order to test a hypothesis (Kalof, Dan, & Dietz, 2008). The use of surveys is also instrumental in determining any potential links or relationships between variables, traits and/or behaviours (Kalof et al., 2008).

This method of data collection will help an online shopping company determine what methods or actions are most useful in helping to retain their customer base after a data breach.

Research Design

The first part of the questionnaire will focus on understanding who an online shopper is and identifying any potential trends amongst online shoppers. The second part of the questionnaire will focus on a hypothetical case study in which the respondent will assume the role of a customer that has been affected by a data breach after using the services of a fictitious online shopping company and as a customer that has not been affected directly but utilises the services of a company that has suffered a data breach. The respondent will answer predetermined questions about various methods or actions an online shopping company can use with the aim of retaining the customer. Creswell (2003) defines case studies as a tool in which to analyse respondent's activities and answers over a specified time period. Various data collection methods can be used, such as questionnaires. The questions utilised on the questionnaire will be close-ended. Close-ended questions are questions whereby respondents answer from pre-determined choices, making it a lot easier to quantify (Kalof, Dan, & Dietz, 2008). Furthermore, the use of close-ended questions is usually a lot easier for respondents to answer as respondents do not need to seek assistance in answering them (Kalof et al., 2008).

The use of questionnaires provides an easy method to collect data within a limited time frame, however, if the questionnaire is poorly structured inaccurate information can be obtained. Furthermore, a poor response rate from respondents can, in fact, negate an accurate reflection of the population sample, thereby hindering the accuracy of findings. Incomplete questionnaires from respondents can impact negatively on the results as well.

Population

According to Kalof et al. (2008), a population is a collection of people that share a standard feature or interest. As the demographics of an online shopper has evolved to the stage where anyone can be an online shopper (Grau, 2005), it is

feasible to select a wide variety of people in order to reflect an accurate population. Additionally, technology has evolved to the point where customers can now utilise mobile devices such as smartphones and laptops to shop online. As mobile penetration is increasing worldwide the potential number of online shoppers has increased (Smith, 2017).

A questionnaire in the form of a survey will be used to gather data and will be sent electronically to a wide variety of people. As online shoppers can potentially be anyone, it is tough to distinguish who they are, and for the purpose of this study, these surveys will be sent to a wide variety of people from various backgrounds. One hundred and fifty questionnaires will be employed in order to conduct this research.

Research Instrument

A structured survey questionnaire with predetermined questions is utilised for this study and will consist of the following sections. (Please see attached appendix)

1) A covering letter – which will provide the context of the study, and the purpose of the study, and ensure recipients that the data they provide will remain confidential
2) The Survey – The survey is divided into two parts.
    a) Part A will require respondents to answer various predetermined questions relating to their online shopping habits and seeks to determine whether they have ever been a victim of a data breach and their experience in dealing with online shopping companies. These questions also seek to identify potential trends.
    b) Part B will require respondents to answer predetermined questions and imagine themselves in various hypothetical scenarios in order to determine what techniques or attributes would convince them to remain as online shoppers for an online shopping company that has experienced a data breach. The following attributes, an apology, technical assistance, legal assistance, compensation and a full refund will be tested and presented to respondents in various combinations.

The data collected from the surveys will help confirm that an online shopper can be anyone. Furthermore, the data collected will help online shopping companies determine which methods and actions could potentially assist them in retaining their customer base, in the event of a data breach.

Data Analysis & Interpretation

Firstly, data collected from the first part of the survey, descriptive data, will be used to provide demographic information about online shoppers, this will be represented in the form of pie charts and bar graphs. The descriptive data collected will also help identify any potential trends amongst those respondents who shop online. The second part of the survey seeks to determine which attribute or combination of attributes will best help an online shopping company retain its customer base after a data breach. Conjoint analysis will be used to analyse the data from the second part of the questionnaire. Conjoint analysis is a marketing technique used to measure the effectiveness of a service that uses different attributes or methods. This technique can provide information concerning the impact of the attribute or method and determine whether it will have a positive or negative effect (Dobney, Ochoa, & Revilla, 2016).

Validity

The external validity of this study is high, as a wide variety of people from several backgrounds are included in the sample. This should contribute to a well-represented sample. The use of close-ended questions within the questionnaire will significantly help in reducing any potential confusion. The questions on the questionnaire are simple and easy to understand, which will help when drawing conclusions from the results. A standardised survey will be employed and sent to all respondents in order to establish a level of firm consistency. The questions are based on the various methods discussed in the literature review.

Reliability

In order to ensure reliability, a standardised questionnaire will be sent to all respondents. Additionally, the questionnaire will be tested in several pre-trials in order to remove any potential stumbling blocks. The more consistent findings are over time, the more reliable they become (Kalof et al., 2008). All answers to

questionnaires will be handled confidentially, in order to maintain standards of ethics.

5. Analysis and Discussion of Results

The data collected from this survey is experimental, and the findings gathered from this survey do not necessarily represent the entire population. One hundred and fifty respondents were recorded out of the required 150. As data breaches are occurring more frequently online shopping companies need to explore methods or options they can offer customers when a data breach has occurred. The sample surveyed were asked to score whether any attribute or action provided by the online shopping company could possibly overcome the impact of the data breach and convince them to continue shopping online at the same company. Several attributes were identified and tested against the sample. These attributes included the issuing of an apology to those affected by the data breach; the offer of free technical assistance to those affected, the offer of free legal aid to those affected; the offer of some compensation to those affected and finally a full refund to those who were affected by the data breach. Additionally, descriptive data collected from the sample population will be used to identify potential trends and behaviour amongst online shoppers.

Of the sample surveyed, males constituted 48% and females 52% of the survey. Participants who were 30 and younger represented 25% of the sample size. Participants aged 31 – 35 represented 26.32% of the sample size as well as participants aged between 36 – 40, who also constituted 26.32% of the sample size. The remaining 22.37% of the sample size fell into the 41 and older category. 91.45% of the sample size said they shopped online, while the remaining 8.55% said they did not shop online at all (See Figure 4).

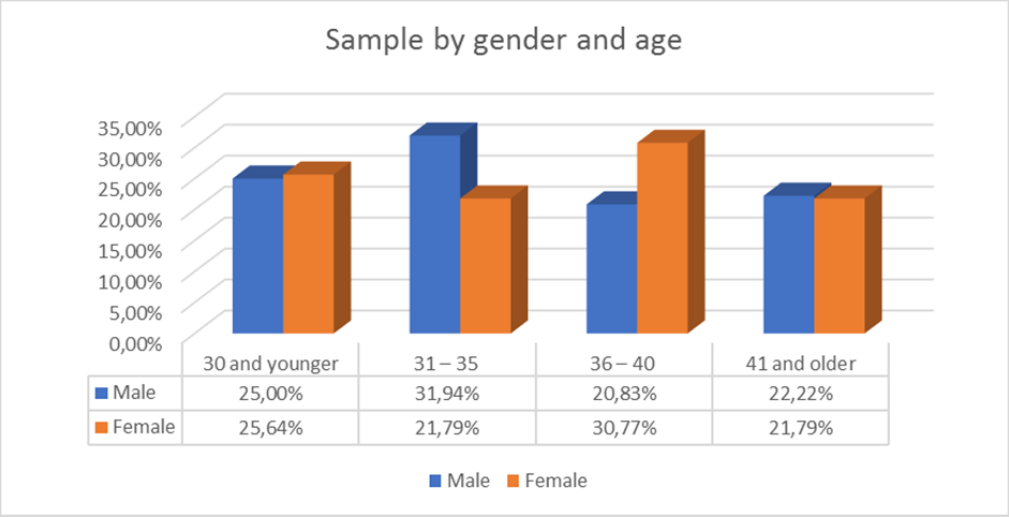


Figure 4: Sample size by gender and age

Device Preference

According to Lee (2016), mobile commerce has become the new method of shopping online. Mobile commerce is defined as the exchange of goods via transactions through a wireless telecommunication network. The convenience that it provides has made this method more popular, primarily through devices such as laptops and smartphones (Lee, 2016). Interestingly, data collected from the survey indicated that laptops and smartphones were the most popular devices used by participants in the survey when they shopped online. 42.07% of respondents used laptops, 33.21% preferred Smartphones, 11.81% used tablets and 11.44% used Desktop Computers. 1.48% used other devices (See Figure 5)

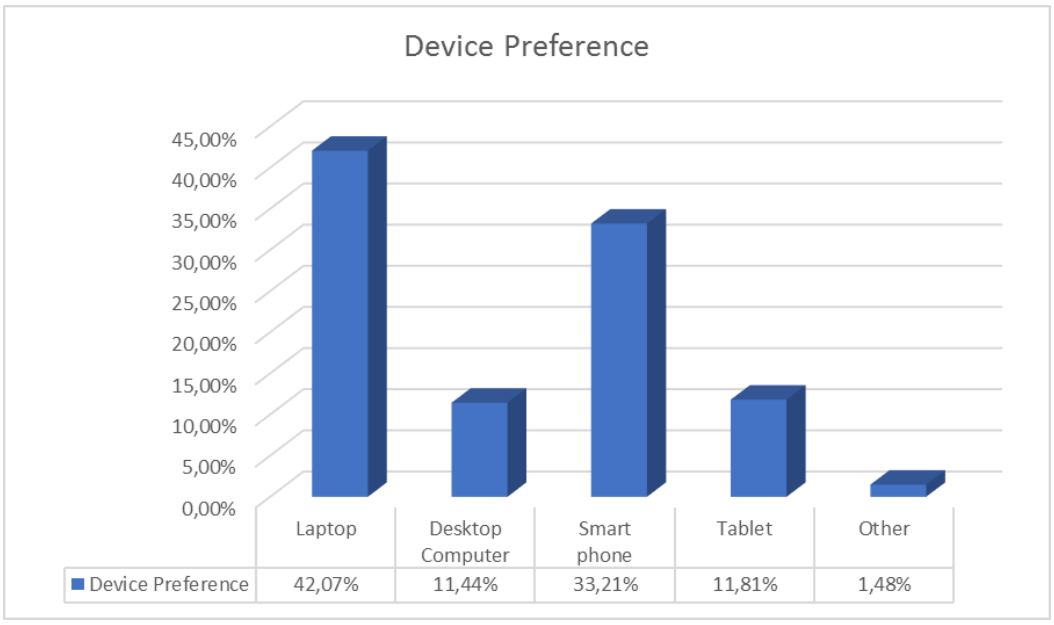


Figure 5 Device Preference of the sample

Surprisingly, a large number of respondents used more than one device when shopping online. 48.83% used two devices, 30.23% used only one device, 16.27% used three devices while the remaining 4.65% used four devices when shopping online (See Figure 6).

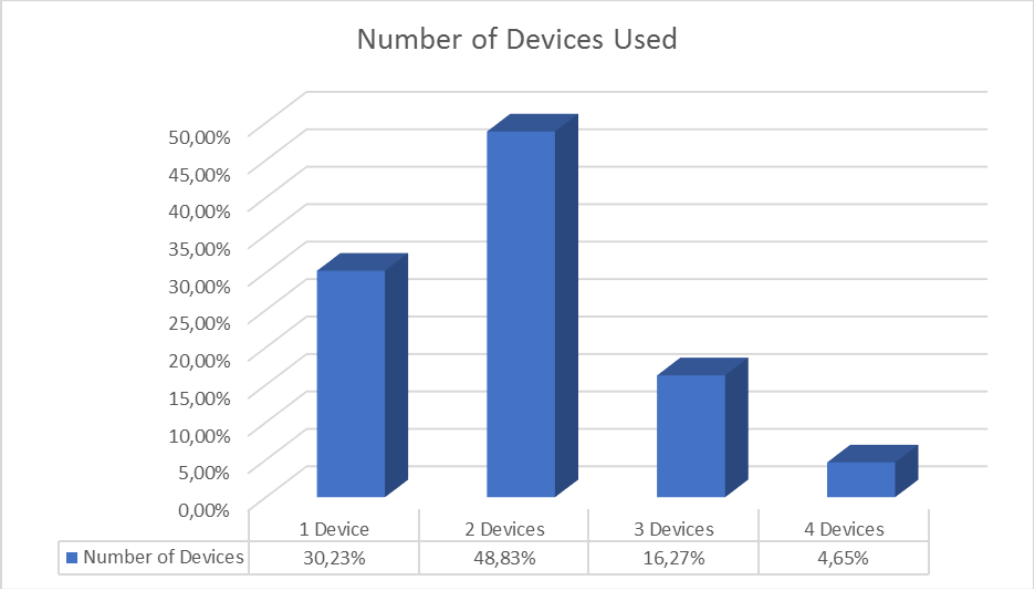


Figure 6 Number of Devices Respondents use in online shopping

Interestingly, the majority of respondents used two devices when shopping online, laptops and smartphones were the more popular devices. These mobile devices have allowed people easier access to the online market. As mobile penetration increases throughout the world, especially in South Africa for example, the number of potential consumers has increased significantly (Tech Central, 2017). According to Tech Central (2017), online spending in general via mobile devices increased by roughly 65% between 2015 and 2016. Analysts have forecasted a continued increase in this trend. Mobile expenditure provides consumers with unlimited spatial constraints, allowing them to access online shopping platforms from anywhere (Lee, 2016).

When analysing data collected from the survey by age in the device preference category, mobile devices such as laptops and smartphones appear to be more popular amongst all age groups (See Figure 7).

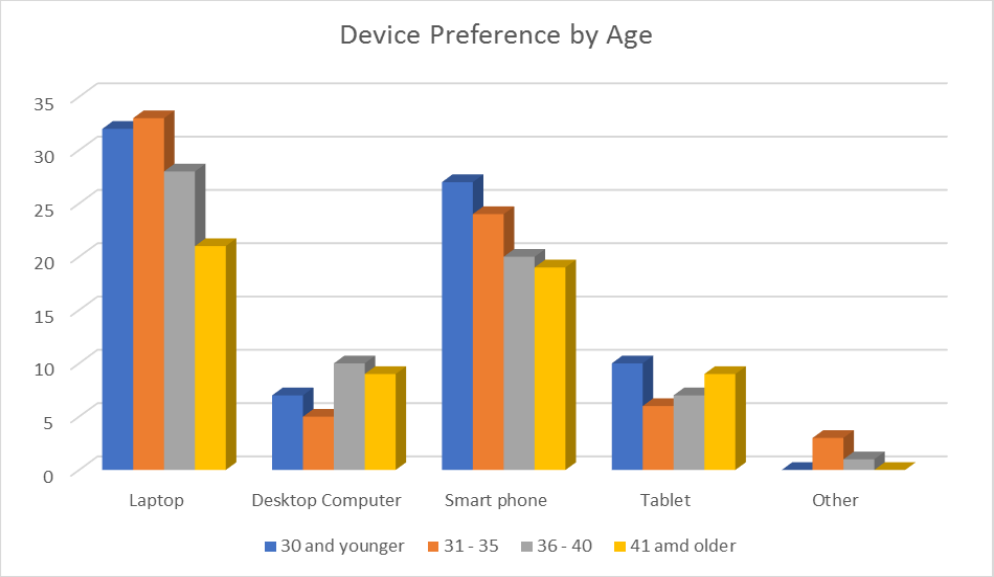


Figure 7 Device Preference by age

Additionally, this trend is seen again when breaking the same data by gender. Mobile devices seem to be more popular than the traditional fixed devices such as desktop computers (See Figure 8)

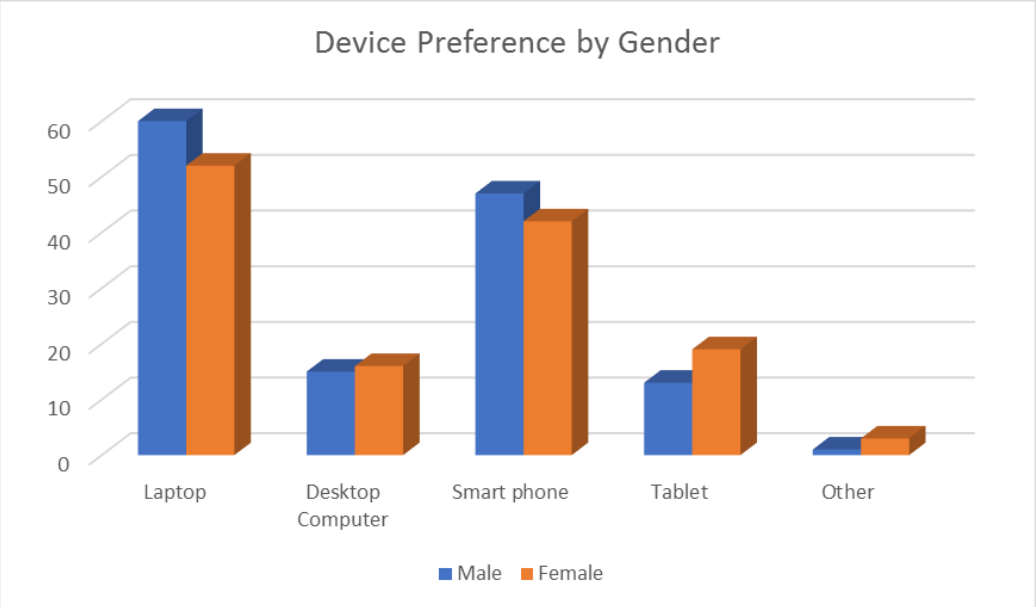


Figure 8 Device Preference by gender

The Motivation for Shopping Online.

According to Sethi and Sethi (2016), convenience is the main reasons customers shop online. Customers are able to access the website and shop at all hours of the day and night at the comfort of their own home or in some cases via their mobile devices as they are not physically able to go to a store. Additionally, online

shopping provides customers with the ability to quickly compare prices of similar products at the click of a button (Sethi & Sethi, 2016). Not surprisingly, the online convenience shopping provides, was the main reason respondents shop online. 37.69% of respondents said they shopped online for convenience, while 21.58% claimed there was better pricing available. 19.45% said there was a more extensive range of products available and 17.93% said they shopped online to avoid buying at a store physically. 3.34% said they shopped online for discretion (See Figure 9)

Figure 9 Reasons for shopping online

Interestingly, when comparing the same data collected from the survey by age groups and by gender, the results were very similar. Convenience was undoubtedly the main reason for shopping online. Numerous online shopping companies adopt various strategies in order to attract customers, focusing on competitive pricing and the speed of delivery (Gerbig, 2017). Ultimately this can lead to customers using more than one online shopping platform. According to the data collected 92.81% of respondents used multiple online shopping platforms when shopping online, while the remaining 7.19% did not (See Figure 10)

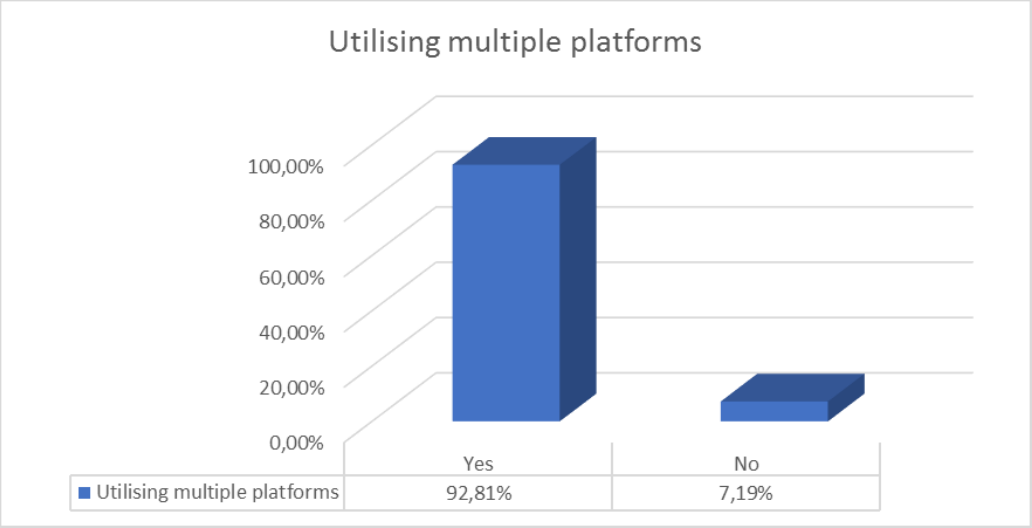


Figure 10 Respondents who utilise more than one platform

When comparing the data by gender (See Figure 11) 89.55% of males said they used multiple online shopping platforms while the remaining 10.45% did not. 95.71% of Females said they utilised numerous platforms and the remaining 4.29% did not.

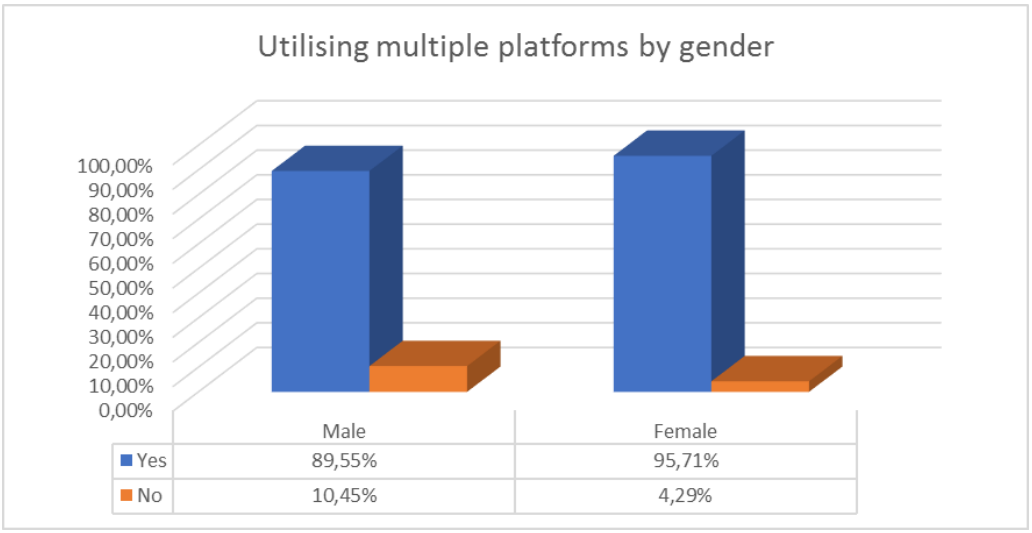


Figure 11 Respondents who utilise more than one platform by gender

There were also similar findings when comparing the data by age group. Ninety-one-point eighty-nine percent of respondents in the 30 and younger age group, and the 31 – 35 age group used multiple platforms for shopping online, while the remaining 8.11% in both age groups did not. In the 36 – 40 age group 88.88% of respondents used multiple platforms when shopping online, while 11.12% did not. In the 41 and older category all respondents used numerous platforms when buying online (See Figure 12).

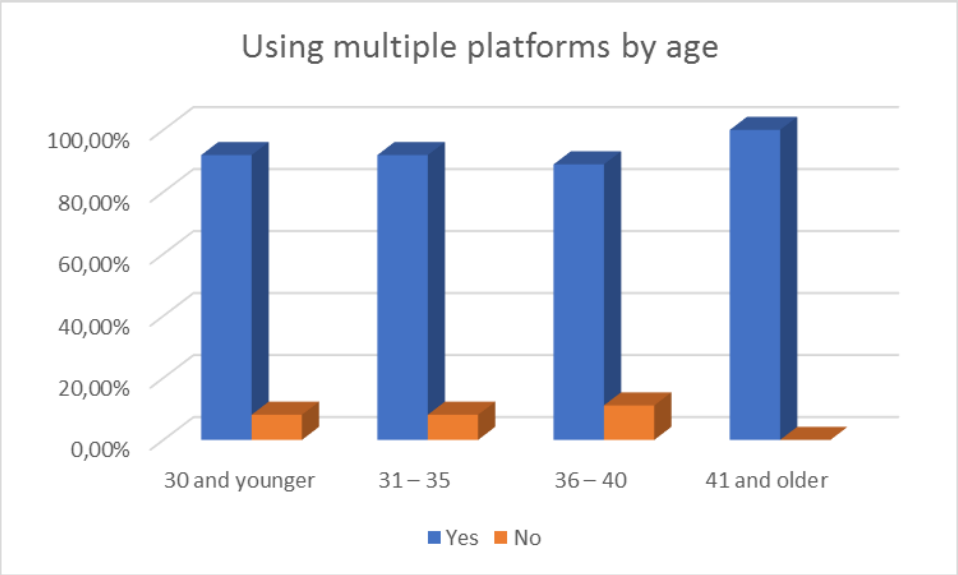


Figure 12 Respondents who utilise more than one platform by age

The Frequency of Online Shopping

The rate of online shopping varied amongst the respondents 38,41% of respondents from the survey tended to shop at least once a month, while 33.33% of respondents tended to shop online every three months. 22.46% tended to shop once a week and 5.07% shop online once a year. Only 0.72% shopped online once a day.

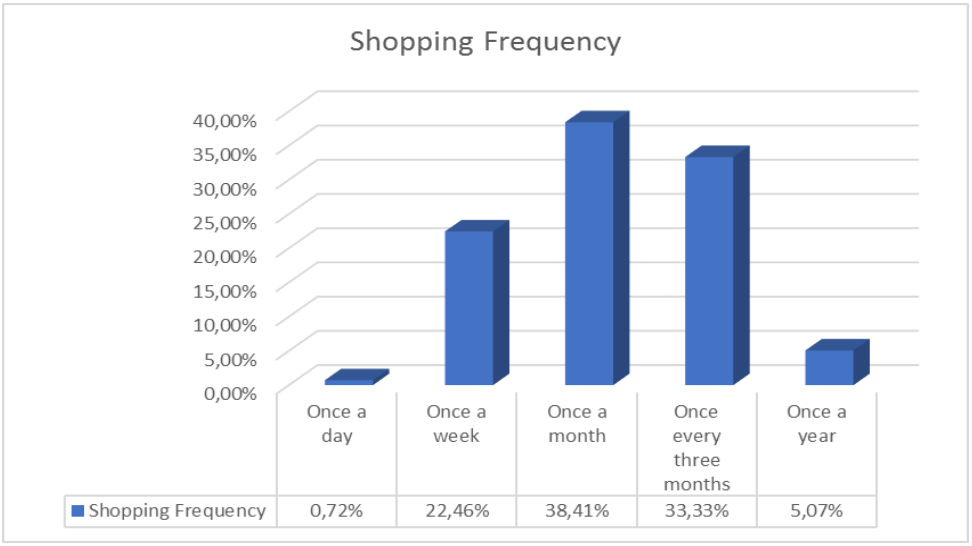


Figure 13 Shopping frequency of respondents

When analysing the same data by age groups, there were a lot of similarities. However, when comparing the data by gender, 43.48% of females shopped online once a month compared to 31.34% of males who also shopped once a

month. 40.29% of males shopped online once every three months compared to 27.54% of females who also shopped online every three months (See Figure 14).

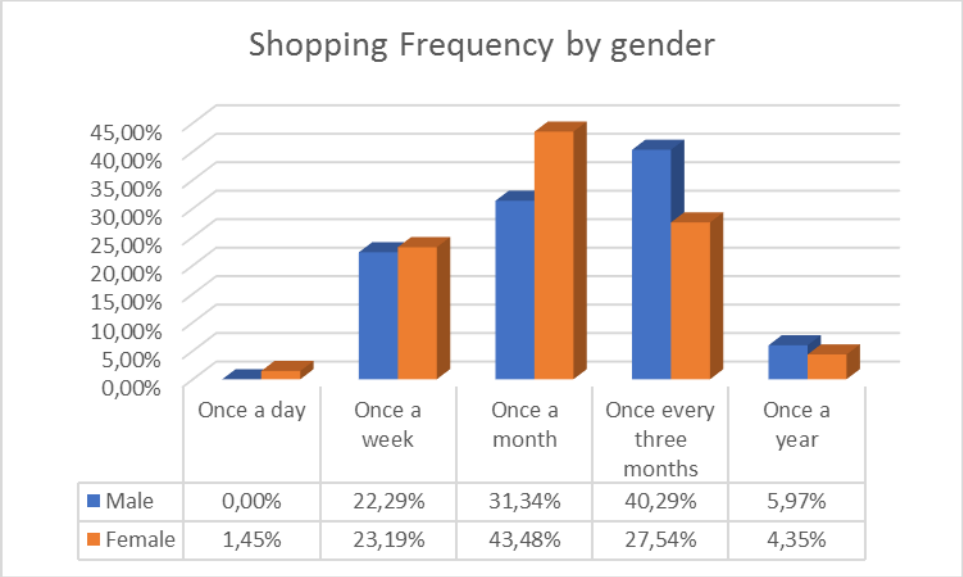


Figure 14 Shopping frequency of respondents by gender

Cybercrime

As discussed earlier, cybercrime is increasing annually, and anyone who accesses the internet is susceptible to cybercrime. Cybercrime is considered one of the biggest threats to online shopping companies, but also the perceived risk of cybercrime. Of the participants surveyed, 13.67% were a victim of a cybercrime, while the remaining 86.33% were not (See Figure 15).

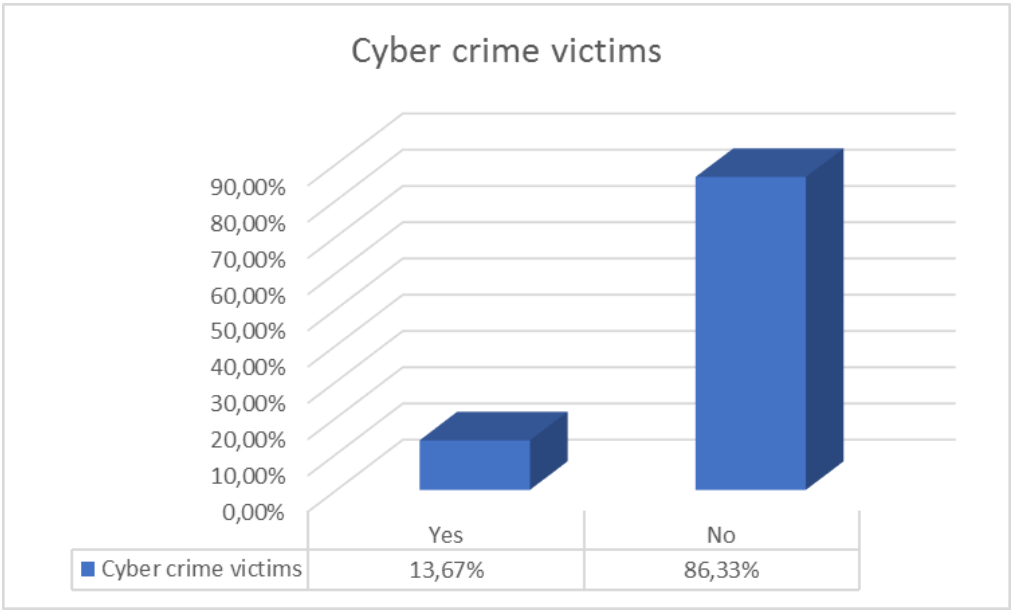


Figure 15 Victims of Cybercrime

According to the data collected by the sample, the majority of cybercrime victims fell in the 36 – 40 and 41 and older age group. According to the table below (Figure 16), males were more susceptible to cybercrime than females. 14.93% of males and 12.86% of females surveyed were victims of cybercrime. Interestingly the difference was quite small.

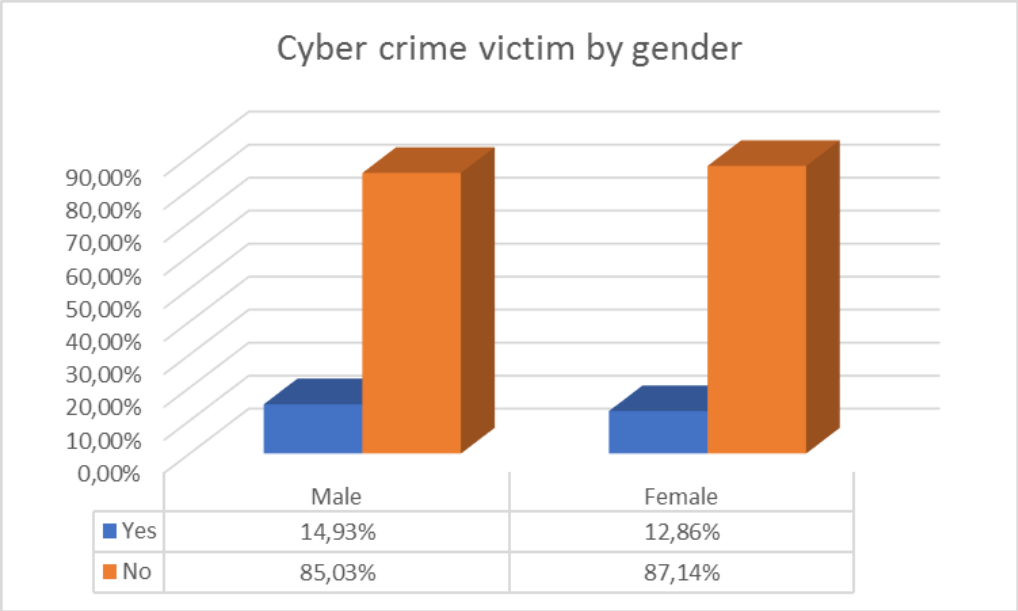


Figure 16 Victims of cybercrime by gender

Interestingly, the data indicated that people in older age groups were more susceptible to cybercrime than those who were younger, when comparing the data by sex there was no significant difference, as indicated in the table below (See Figure 17). According to Arfi and Agarwal (2013) the elderly, especially those aged 60 and above are more vulnerable to a number of scams. Although they may have the necessary software installed to protect themselves from direct cyber-attacks, the elderly unintentionally fall prey to more direct scams easily. A classic example would be buying cheaper medication online from unscrupulous websites (Arfi & Agarwal, 2013).

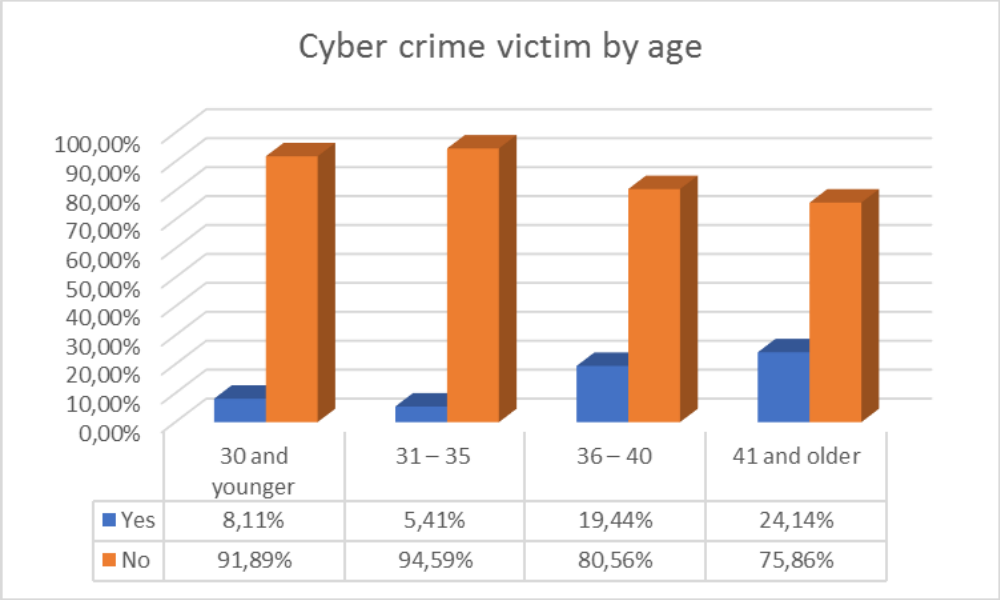


Figure 17 Victims of cybercrime by age

Cybercrime comes in various forms, 71.43% of respondents who were a victim of cybercrime had their personal and financial information compromised by a data breach. 4,76% of respondents fell victim to a Malware scam. No one surveyed fell victim to a ransomware scam, and the remaining 23.81% fell into the 'Other' cybercrime category (See Figure 18)

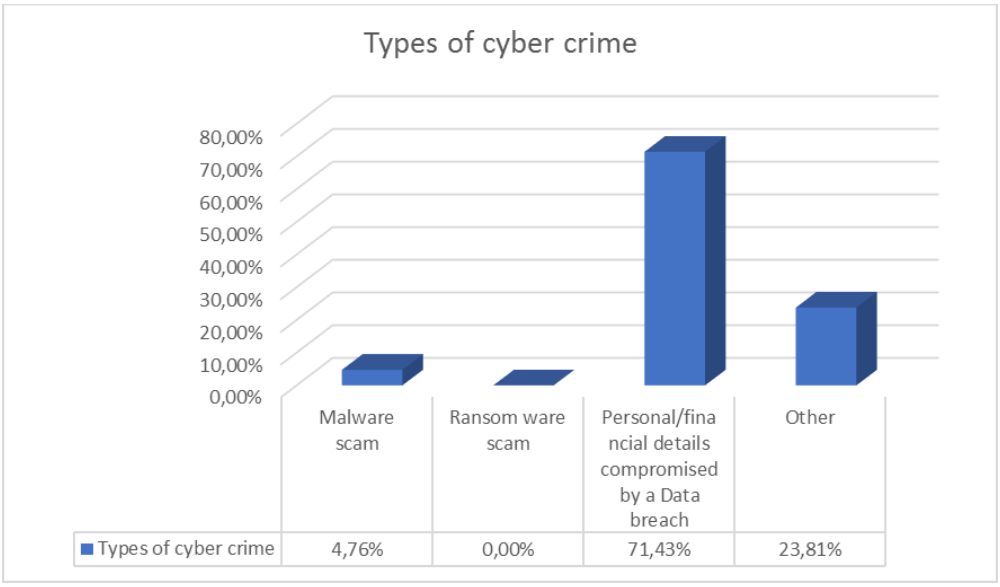


Figure 18 Types of cybercrime

Of the 23.81% who fell into the Other category (See Figure 19), 60% were victims of credit card fraud, 20% were victims of phishing scams. A phishing scam is defined as an attempt by a hacker to obtain personal and financial information from a victim via a scrupulous email, and the remaining 20% were a victim of an employee data breach from within a company. Employee data breaches are

known to happen from time to time. In some cases, the employee who commits the cybercrime is often a disgruntled employee. According to Ogden (2016), employees who intentionally compromise the data accounts of customers do so because of being terminated from their position or they do it for career building opportunities (Ogden, 2016).

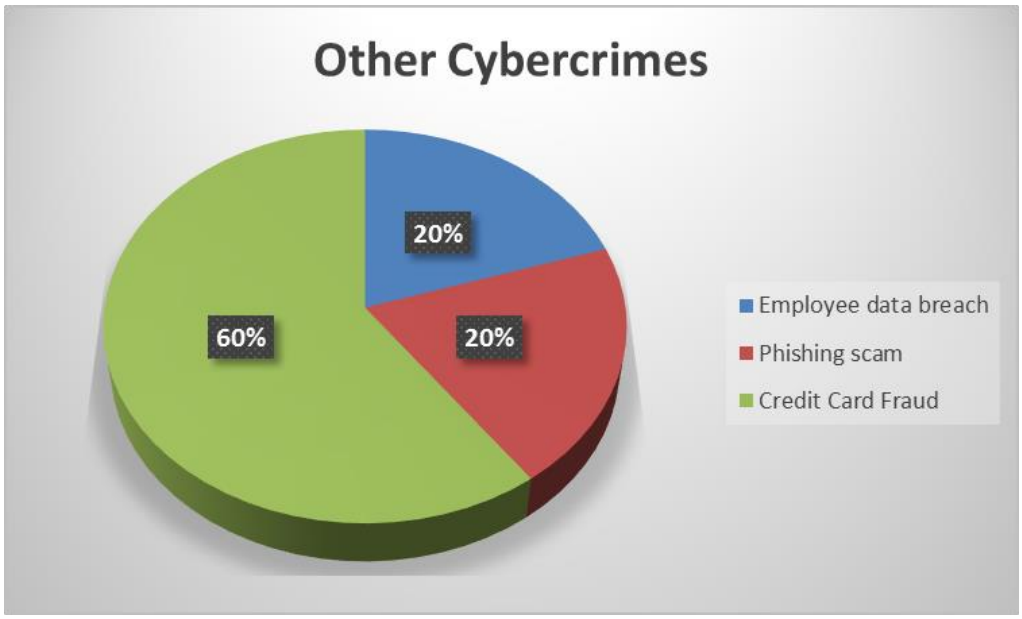


Figure 19 Other Cybercrimes

Not surprisingly, all the victims of cybercrime from the survey reported the cybercrime to their respective companies. Yet, 11.11% of those affected were informed of the incident by the respective companies they shopped at (See Figure 20)

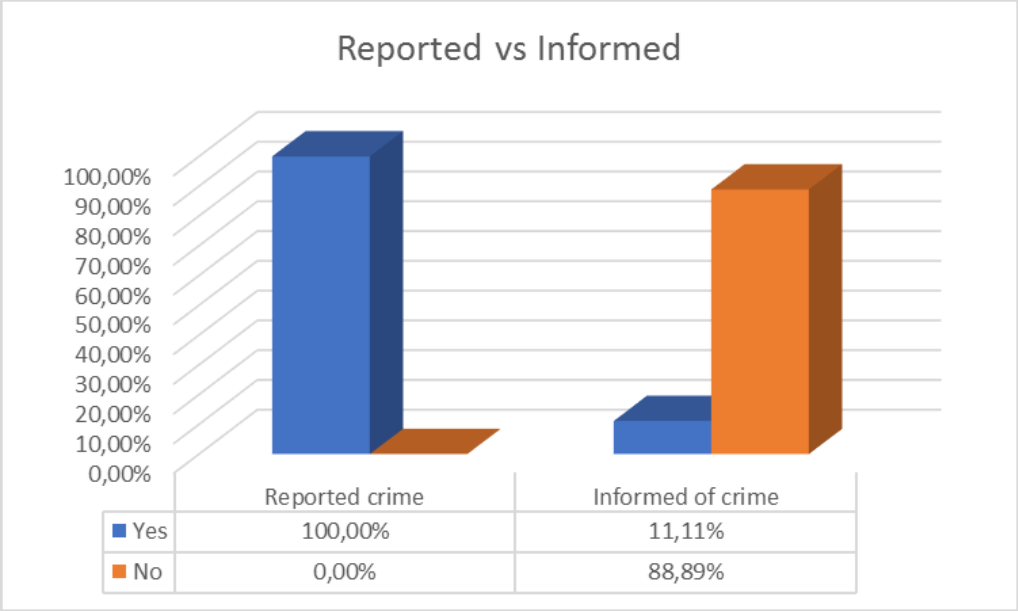


Figure 20 Cybercrime victims who were informed vs reported

Some companies fail to disclose data breaches due to the potential loss of further revenue and because of the potential damage to the reputation of the company. Data breaches are a financial and reputational catastrophe for companies affected, and most companies find it a lot easier to hide the data breach from their customer than actually revealing the truth. The reasoning behind this according to Drinkwater, (2016) is that a loss of customer loyalty equates to a loss in business for the company and decline in share price, it also affects the brand reputation of the company. Additionally, the longer the data breach is concealed from customers, the more significant the negative impact will be when news of the data breach breaks. (Drinkwater, 2016).

However, according to Skroupa (2016), several companies are prepared to risk the consequences of hiding a data breach than revealing the breach to its customer base, because of the potential loss of intellectual property and competitive advantage in the market. Typically, in the event of a breach, customers look at competitors as an alternative (Skroupa, 2016). Additionally, legislation that governs companies over revealing data breaches is comprehensive and lax and differs from country to country (Freifeld, 2014).

Overall, 55.56% of respondents who were a victim of cybercrime were not satisfied by the service they received from the company, as opposed to the 44.44% of respondents who said they were satisfied (See Figure 21).

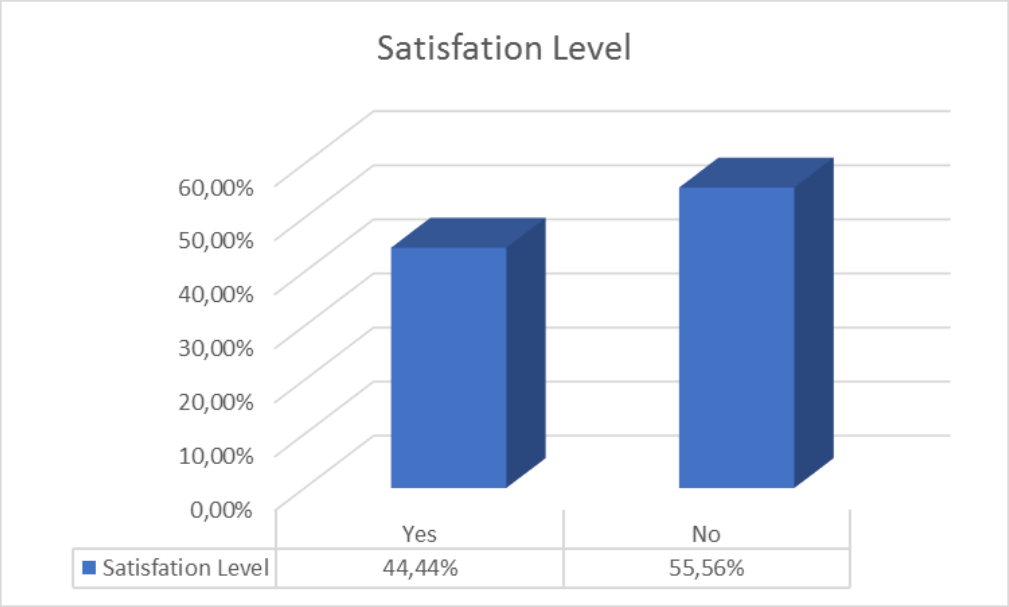


Figure 21 Cybercrime victims level of satisfaction

Interestingly, when comparing the satisfaction level against those respondents who were informed and not informed, the results yielded interesting results. All respondents who were notified of the incident were satisfied by the service they received from the company. However, those respondents who were not informed were split. 37.5% of respondents who were not notified of the incident were satisfied by the service they received from the company, yet the remaining 62.5% of respondents who were not informed of the incident were unsatisfied by the service they received from the company (See Figure 22).

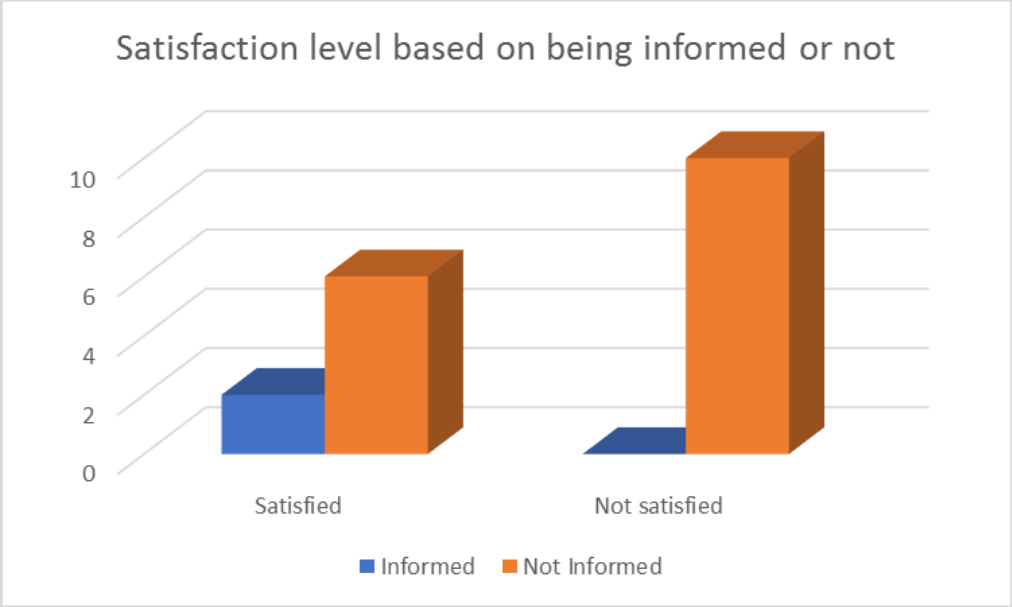


Figure 22 Cybercrime victims satisfaction level based on being informed or not

In most cases, unsatisfied shoppers will not utilise the services of a company where they had a bad experience again. As a result, this bad experience has an adverse effect on the reputation of the business and has the potential to destroy customer trust. However, the data collected from the survey indicates that of the respondents who were victims of cybercrime, 89.47% trust the websites of online shopping while the remaining 10,53% do not trust the site. Interestingly 95% of respondents who were not a victim of a cybercrime trusted the websites, while the remaining 5% did not trust the website they shopped at (See Figure 23).

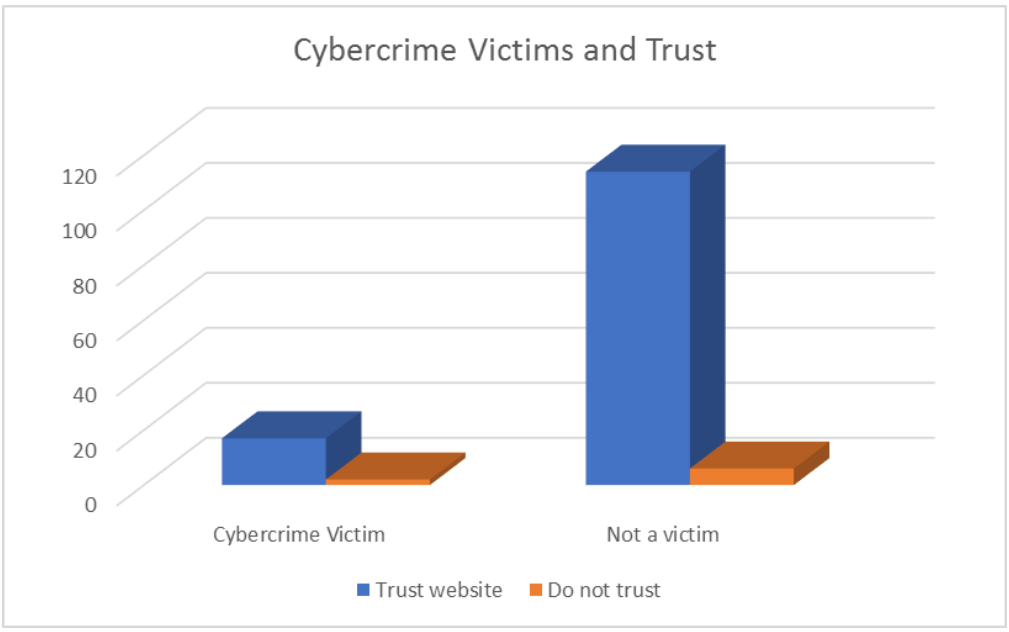


Figure 23 Level of trust amongst cybercrime victims and non-victims

Responding to Data Breaches

Companies need to protect their customers or risk losing them to their competitors. Customers need to be able to trust the company they are using. Additionally, in the event of a data breach, customers want the company to be accountable and to explain what went wrong (Lieberman, 2017). Customer satisfaction and retention are critical components to the long-term success and survival of a company

The Use of an Apology

The use of an apology is usually the first step to take whenever a crisis hits business and affects its customer base. According to Andersen (2012), leaders who do apologise are courageous. These leaders, by apologising are in fact admitting that they failed. Andersen (2012) argues that it is essential for leaders of businesses to be open and frank with their customer base when they have faced a crisis. Kellerman (2006) explains that by not apologising, more harm will come than good, and states that apologising is an attempt by a leader to put their mistakes behind them. However, apologies are multi-faceted, they are issued in order to gain forgiveness for any wrongdoing, and are shaped by the culture in which one operates, and can appeal to people but at the same time can have the opposite effect and repel those who were affected (Kellerman, 2006). Thus, in some cases, apologies can be interpreted as an admission of guilt by some affected consumers.

When testing the attribute of an apology only to those affected by a data breach in the survey, only 0.8% of the respondents, reacted positively to it (See Figure 24). This data suggests that an apology on its own did not have a positive impact at all. Interestingly, when not responding to those who were affected by a data breach only 0.8% of respondents reacted positively (See Figure 24)

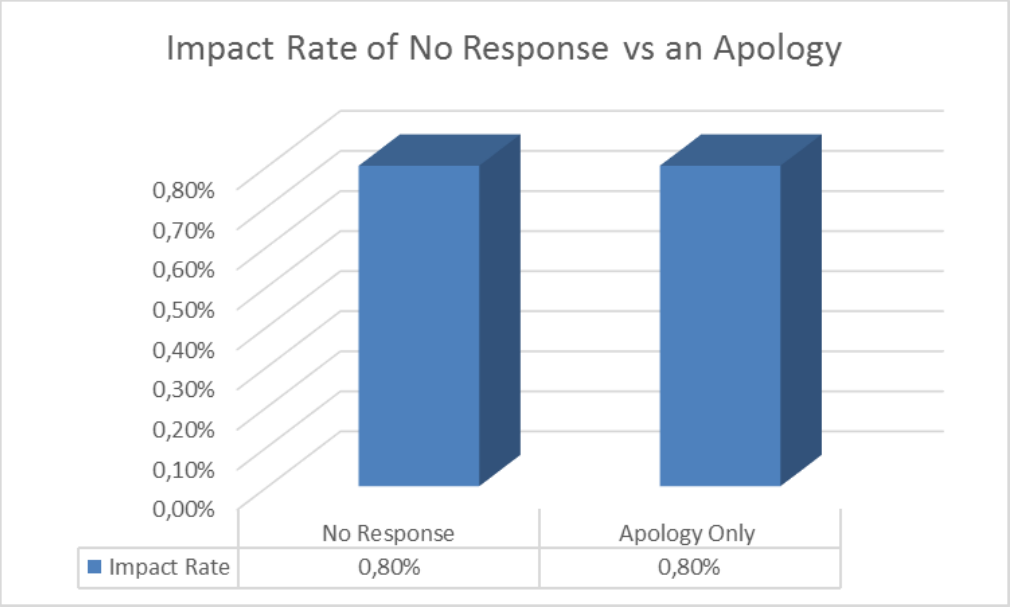


Figure 24 Impact rate of no response vs an apology

Trust in a particular product or service is an essential attribute of customers. Trust can potentially influence a consumer's willingness to shop at a specific place for a particular brand. Additionally, trust in the security of the website is fundamental to consumers who utilise online shopping platforms (Olenski, 2016). In the online shopping sphere, customers rely heavily on trust, when making a decision. This trust is placed in the website which they decide to utilise when purchasing online.

The data from the surveyed respondents depicted in (Figure 25), shows that 5.76% of respondents did not trust the online shopping website they chose to use. However, a large number of surveyed respondents 94.24% said that they did trust the platforms they shopped at. As trust is a massive contributor to consumer's decision to shop online, it is unsurprising that the confidence a customer had in a particular online shopping company is broken in the event of a data breach.

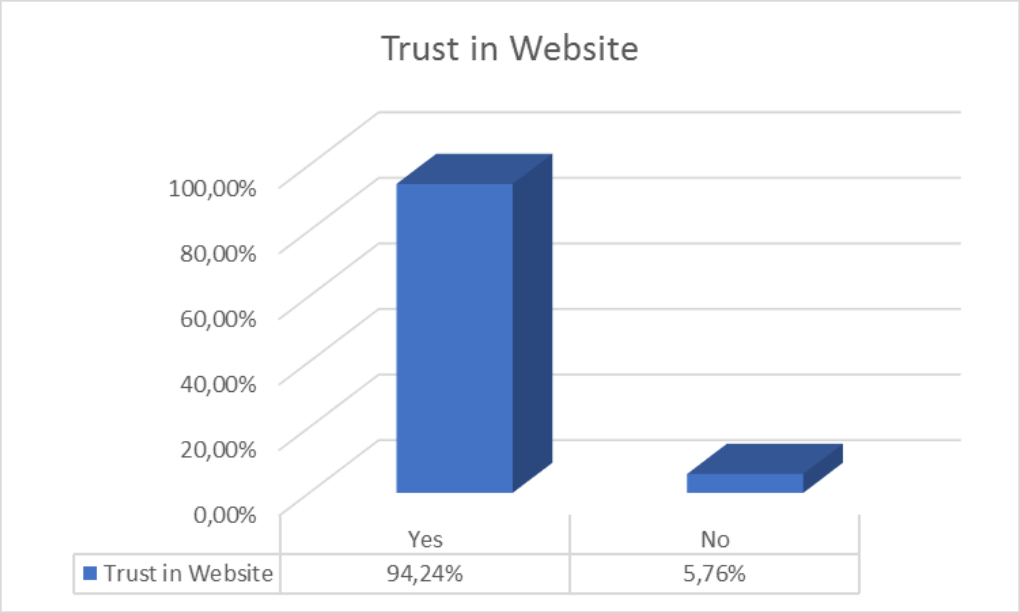


Figure 25 Respondents trust in the website

Retaining the Customer Base

According to Professor Jagdip Singh, a marketing academic based at the Weatherhead School of Management at Case Western Reserve University in the United States, offering a customer an apology is entirely counterproductive. Businesses should instead provide customers affected by lousy service with different options and solutions instead. An apology on its own, means there is no solution, it can be interpreted as this is the only option a customer will receive (Harvard Business Review, 2018).

Interestingly, when offering customers affected by a data breach with different attributes, the impact varied, depending on what options were provided to customers. When customers were offered an apology coupled with free legal assistance, only 2.4% of customers affected by a data breach responded positively.

When customers were offered an apology, free technical and legal assistance, 9.5% of customers who were affected by a data breach responded positively. According to Liberman (2017), companies should offer complementary services such as providing technical advice to customers on how to better protect themselves from cyber threats in order to give them a sense of control over how

their data is managed. Additionally, companies should hire outside well-known consulting firms to help test the system, in order to prevent further attacks.

When customers were offered an apology, free technical and legal assistance coupled with some compensation, the impact increased to 27.8%. Compensation does provide a positive impact on customers affected. However, it is challenging to gauge the amount of compensation needed in order to satisfy customers. (Goode, Hoehle, Venkatesh, & Brown, 2017). Compensation can be viewed as a gift. But the gift companies offer to their customers affected by the data breach must add value, such as offering 50% off their next purchase. No customer is going to accept compensation or a gift that will not add value (Ariely, 2008). In this case, only some compensation was offered, and although it had a positive effect, the vast majority of customers were still unhappy with what was being offered. Interestingly, when customers were offered an apology, free technical assistance and full compensation, the impact increased significantly to 41.3%. The effect of full compensation had an even more significant impact than some compensation. Although not all customers affected are satisfied, the effect was quite significant.

When customers were offered an apology, free technical and legal assistance and a full refund the impact increased positively to 49.2% of the respondents. A full refund to customers provides a significant impact on customers. As a data breach can possibly result in a loss of finances for customers, reimbursing them for their loss is vital in rebuilding trust (Haesevoets, Hiel†, Pandelaere, Bostyn†, & Cremer, 2017). However, despite including a full refund, roughly more than half of the respondents reacted negatively (See Figure 26)

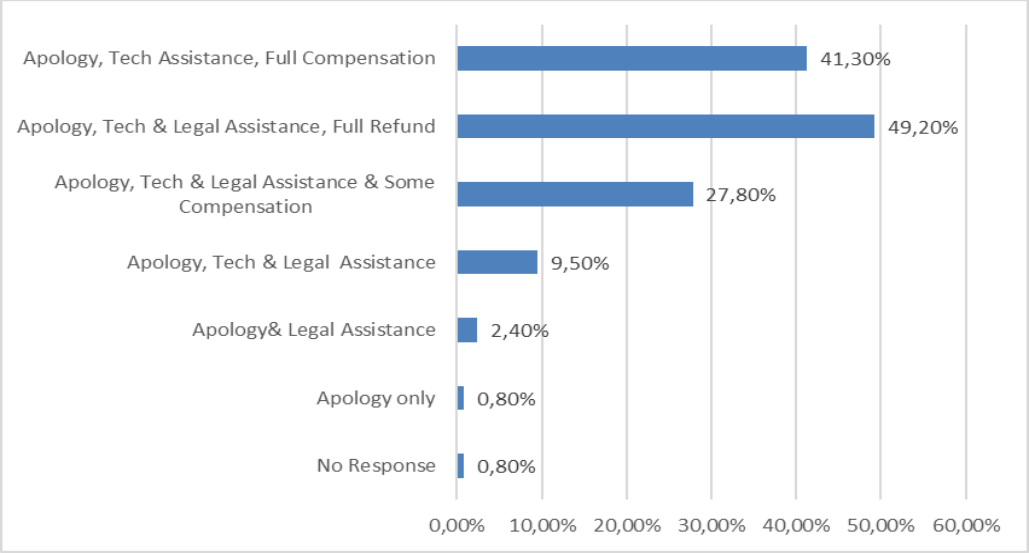


Figure 26 The impact of the attributes or options

Findings

When testing what attributes or options would have a positive impact on customers affected directly by a data breach, it was found that a combination of attributes or options is needed in order to gain maximum impact. An apology is an essential tool for a business in the event of a data breach. However, an apology on its own did not have a positive impact on the participants that were surveyed. In some cases, an apology can be viewed as an admission of guilt. Ideally, an apology needs to be issued with other attributes or options in order to have any positive impact at all. Proposition 1 – No response from an online shopping will have a positive effect on customers who are affected by a data breach. There was no significant positive impact at all. Only 0.8% of respondents reacted positively Proposition 2 - An apology on its own will have a positive impact on customers who are affected by a data breach. Similarly, this attribute on its own did not have a significant positive impact at all. Only 0.8% of respondents reacted favourably.

Offering complimentary technical and legal assistance will help address the questions most customers ask. Most customers want to know how the data breach occurred and will look to the company for answers. Companies must be in a position to answer these questions and address concerns about further potential breaches. Additionally, free technical assistance can be used to help customers mitigate their risk of data breaches. However, despite this need to

understand how a data breach occurred, this attribute in combination with an apology had little positive impact. Proposition 3 – An apology and free legal assistance will have a positive impact on customers affected by a data breach. There was a minor positive impact from respondents. Only 2.4% of respondents reacted positively. Overall this combination of attributes did not have a significant positive impact at all on respondents. Proposition 4 – An apology, free technical and legal assistance will have a positive impact on customers affected by a data breach. There was a slight positive improvement, with only 9.5% of respondents reacting positively. Overall this combination of attributes did not have a significant positive impact at all.

When offering compensation, the positive impact increased significantly. However, it is complicated to gauge how much compensation is needed in order to satisfy all customers affected by a data breach. Some customers may be happy with a set amount while others may feel insulted by the amount. Proposition 5 – An apology, free technical and legal assistance and some compensation will have a positive impact on customers affected by a data breach. There was a significant increase, with 27.8% of respondents reacting positively. Overall this set of attributes will help have a positive impact, yet the majority of respondents were still unhappy. Proposition 6 – An apology, free technical assistance and full compensation will have a positive impact on customers affected by a data breach. Overall 41.3% of respondents reacted positively to this combination, yet over half the respondents were still unhappy.

Ultimately, companies need to refund their customers for any damage and loss of financial and personal information, in order to gain the best positive impact. However, some smaller online shopping companies may not be in a financial position to do so. Proposition 7 – An apology, free technical assistance and full compensation will have a positive impact on customers affected by a data breach. This combination of attributes yielded the most substantial positive impact with 49.2% of respondents reacting positively. However, just over half of the respondents were still unhappy.

Despite offering all available options to customers that have suffered from a data breach, it is unlikely that an online shopping company will be able to retain all of its affected customer base. Hypothesis - Following a data breach in which the financial and personal data of customers has been compromised, online shopping companies will be able to retain their customer base. Overall online shopping companies will not be able to retain all of their customers. The loss can be negated depending on what attributes online shopping companies offer customers affected by a data breach.

From the survey, of the respondents who were victims of cybercrime and were informed of the incident by the company, all were satisfied with the service they received from the company. Those who were not notified of the incident were split. The vast majority of victims were not happy with the overall service of the company, yet a significant minority were satisfied with the service. Despite that fact that most online shopping companies are unwilling to inform customers of a data breach, the impact is quite severe. However, by notifying customers of a data breach indicates how the company is monitoring the customer's well-being.

Interestingly, the vast majority of respondents who were victims of cybercrime had their personal and financial data compromised by a data breach. Furthermore, the older the respondent was, the more susceptible to a cybercrime they were. However, 89,47% of the cybercrime victims claimed they trusted the website they shopped at.

Mobile devices such as Laptops and smartphones were the most popular devices used when shopping online. Given the daily schedule of people these days and their limited time, online shopping via mobile devices help them shop whilst not actually wasting time going into a traditional store. The continuous development of mobile technology has resulted in mobile devices becoming more popular than traditional devices used for online shopping. Smartphones and laptops are becoming the more preferred devices. This has allowed customers to access online shopping companies more efficiently.

6. Recommendations

Online shopping companies must invest in a comprehensive cybersecurity system and train their staff on the dangers of cybercrime. Not only that, these systems need to be regularly updated, because cybercrimes evolve and cybercriminals evolve their methods as well. Staff need to be continuously retrained on how to deal with these evolving threats.

All companies need to develop a data breach response plan. However, online shopping companies need to go further and run real-time simulations in order to train their staff on what they need to do in order to address the effects of a data breach.

The management and leadership of companies need to change their way of thinking and make cybersecurity an issue of utmost importance. Online shopping companies cannot afford to be reactive to data breaches. They need to become more proactive in militating the threat of data breaches. In the event of a data breach, companies will suffer a loss of revenue and customers, this is inevitable. How these companies respond to data breaches will determine how much of their customer base they can recover. Yet it is essential to understand that a significant number of customers affected by a data breach will never shop online again. Online shoppers are evolving, and evolving technology is facilitating this. Mobile shopping is becoming more popular than the traditional form of online shopping. Online shopping companies need to take this into account and help promote this growth trend, and ensure their platforms are compatible with mobile technology.

7. Limitations

An inadequate response to the surveys may negatively influence the interpretation of the data and compromise the overall results of the research article. The information obtained from respondents was kept confidential and at no time were respondents asked to provide any confidential and financial information such as credit card details. Respondents did not need to provide any personal details at all. This research report did not examine how online shopping companies can improve their cybersecurity methods and practices but instead

tested what attributes these companies can offer and what methods they can utilise to retain their customer base, in the event of a data breach.

8. Recommendations for further studies

As online shopping is evolving due to technological advances, so too is the threat of cybercrime. These new risks will continuously pose a threat to online shopping companies. Overall, online shopping is growing throughout the world and companies need to be able to protect their customer base in order to survive and thrive. Without a comprehensive cybersecurity policy, companies will become easy prey to cybercriminals. However, despite extensive cybersecurity policies and procedures, data breaches do occur. Online shopping companies need to protect the interests of the customers first before they protect the image of the company. Online shopping companies rely on customers to survive, and a dissatisfied customer is a customer that will not return. Therefore, further studies are necessary in order for online shopping companies to test the effectiveness of other attributes or options an online shopping company can use to retain its customer base.

9. Conclusion

Online Shopping started off as a novelty and has grown into a multi-billion-dollar industry that connects people from across the world. Ultimately the concept of online shopping has made the world a smaller place, by allowing a consumer from anywhere in the world access to any product for sale in the world, through any device that can access the internet. The service of online shopping allows customers to shop from the comfort of their home and allows them access to a whole wide range of products, that some customers cannot access from traditional shopping. However, as the reliance on the internet has increased, so too has the threat of cybercrime increased. To date, cybercrime poses the biggest threat to online shopping companies and their customers. In the event of a data breach, companies face the mammoth task of rebuilding the trust of their customer base, especially those customers that have directly been affected by a data breach.

As customers are unable to physically enter the store and interact with staff face to face, a high level of trust is needed between the customer and the online

shopping company. Safe and secure transactions are necessary for customers to continue returning to the online shopping platform in order for the business to thrive. However, in the event of a data breach, the trust between the customer and the company is severely damaged, and in some cases, irreparable Trust is the most pivotal value that is needed for business to be conducted. Repairing trust is no easy task

Data breaches are inevitable, and an online shopping company will always face the potential threat of a data breach, whether facing an external threat or internally from the very employees that work within the company, whether it is intentional or accidental. Investing in proper cybersecurity is essential in helping to protect a company from cybercrime. However, this cybersecurity policy and procedures need to be updated continuously, as cybercrime evolves continuously.

References

Alexander, C. (2015, December 25). What small businesses need to know about cybersecurity. *New Hampshire Business Review, 37*(27), 14. Retrieved November 12, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=6&sid=eef04f78-507c-41e3-9b5c-924fadf08fab%40sessionmgr4008

Alfreds, D. (2016, June 9). *SA business 'unprepared' for cybercrime*. Retrieved September 29, 2017, from Fin 24: http://www.fin24.com/Tech/Cyber-Security/sa-business-unprepared-for-cybercrime-20160609

Andersen, E. (2012, June 5). *Courageous Leaders Don't Make Excuses...They Apologize*. Retrieved March 1, 2018, from Forbes: https://www.forbes.com/sites/erikaandersen/2012/06/05/courageous-leaders-dont-make-excuses-they-apologize/#442f17b64ef8

Arfi, N., & Agarwal, S. (2013, July). Knowledge of Cybercrime among Elderly. *International Journal of Scientific & Engineering Research, 4*(7). Retrieved February 28, 2018, from https://www.researchgate.net/profile/Shalini_Agarwal9/publication/242654499_Knowledge_of_Cybercrime_among_Elderly/links/0deec51cebeac0feef000000/Knowledge-of-Cybercrime-among-Elderly.pdf

Ariely, D. (2008). *Predictably Irrational - The Hidden Forces that Shape our Decisions.* New York: Harper Collins Publishers. Retrieved March 13, 2018

Banham, R. (2017, March 20). *Why Cybersecurity Should Be A No. 1 Business Priority For 2017*. Retrieved September 30, 2017, from Forbes: https://www.forbes.com/sites/eycybersecurity/2017/03/20/why-cybersecurity-should-be-a-no-1-business-priority-for-2017/#50c7017d1719

Barik, P., Soni, V., & Pandey, D. B. (2015, April 1). Online Shopping Catching Up Fast With The Trend- Chhattisgarh Context. *International Journal of Research in Commerce & Management, 6*(4), 53 - 57. Retrieved September 5, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=18180183-1aed-4d6c-8768-eb9ab3ebc887%40sessionmgr4010

Bende, D., & Barnard, K. (2006, January 27). How to Keep Your Customers After a Data Breach. *Business Source Complete, 171*(18), 1. Retrieved September 4, 2017, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/detail/detail?vid=7&sid=e09b5002-d081-4a73-b636-d669ae0c2545%40sessionmgr102&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=19567892&db=bth

Bernard, E. K., & Makienko, I. (2011, January 2). The Effects Of Information Privacy and Online Shopping Experience in E-Commerce. *Academy of Marketing Studies Journal, 15*(1), 97 - 112. Retrieved September 8, 2017, from http://0-

web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=3&sid=432221f1-7d9c-4e53-8304-4ff7b044c98d%40sessionmgr120

Bischoff, P. (2017, July 11). *Analysis: How data breaches affect stock market share prices*. Retrieved October 30, 2017, from Comparitech: https://www.comparitech.com/blog/information-security/data-breach-share-price/

Bourdon, B. (2017, November 20). *The Avoidable Mistakes Executives Continue to Make After a Data Breach*. Retrieved January 8, 2018, from Harvard Business Review: https://hbr.org/2017/11/the-avoidable-mistakes-executives-continue-to-make-after-a-data-breach

Buck, C. (2012, May 16). *Cybercrimes (via cell phones) up in 2011*. Retrieved October 1, 2017, from phys.org: https://phys.org/news/2012-05-cybercrimes-cell.html

Cheng, J. Y.-J., & Groysberg, B. (2017, February 22). *Why Boards Aren't Dealing with Cyberthreats*. Retrieved October 23, 2017, from Harvard Business Review: https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

Choi, B. C., Kim, S. S., & Jiang, Z. (2016, July 1). Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems, 33*(3), 904 - 933. Retrieved September 7, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=7&sid=58237122-2e63-4190-bf0d-800e4e65a562%40sessionmgr4008

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security, 30*, 719 - 731. Retrieved September 7, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/detail/detail?vid=5&sid=2af1b545-deb4-47e9-8ea2-8cd64079b9ef%40sessionmgr4009&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=67246567&db=iih

Creswell, J. W. (2003). *Qualitative, Quantitative and Mixed Methods Approaches.* London: Sage Publications.

Daniel, M. (2017, March 22). *Why Is Cybersecurity So Hard?* Retrieved October 25, 2017, from Harvard Business Review: https://hbr.org/2017/05/why-is-cybersecurity-so-hard

Dennis, M. A. (2017). *Cybercrime*. Retrieved October 1, 2017, from Encyclopedia Britannica: https://www.britannica.com/topic/cybercrime

Disparte, D., & Furlow, C. (2017, May 16). *The Best Cybersecurity Investment You Can Make Is Better Training*. Retrieved October 25, 2017, from Harvard Business Review: https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

Dobney, S., Ochoa, C., & Revilla, M. (2016, December 16). More realism in conjoint analysis: The effect of textual noise and visual style. *International Journal of Market Research, 59*(4). Retrieved January 16, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=4&sid=4cbeb936-c087-45e7-97cd-aa66a41c99a0%40sessionmgr4008

Drinkwater, D. (2016, January 7). *Does a data breach really affect your firm's reputation?* Retrieved October 28, 2017, from CSO: https://www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html

Foltyn, T. (2017, December 28). *Cybersecurity review of 2017: The year of wake-up calls – part 2*. Retrieved January 9, 2018, from We Live Security: https://www.welivesecurity.com/2017/12/28/cybersecurity-review-2017-part-2/

Freifeld, K. (2014, January 16). *U.S. companies allowed to delay disclosure of data breaches*. Retrieved March 8, 2018, from Reuters: https://www.reuters.com/article/us-target-data-notification/u-s-companies-allowed-to-delay-disclosure-of-data-breaches-idUSBREA0F1LO20140116

Geetha, V., & Rangarajan, D. K. (2015, November). A Conceptual Framework for Perceived Risk in Consumer Online Shopping. *Sona Global Management Review, 10*(1), 9 - 22.

Gerbig, C. (2017, October 3). *E-Commerce Done Right: Five Keys To A Successful Online Business*. Retrieved March 8, 2018, from Forbes: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2017/10/03/e-commerce-done-right-five-keys-to-a-successful-online-business/#2e60823248ee

Girish, M., Chandukala, S. R., & Liu, Q. (2016, March). Exploring the Effects of "What" (Product) and "Where" (Website) Characteristics on Online Shopping Behavior. *Journal of Marketing, 80*, 21 - 39. Retrieved September 18, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=8&sid=2af1b545-deb4-47e9-8ea2-8cd64079b9ef%40sessionmgr4009

Goldberg, E. (2013, June 1). Preventing a data breach from becoming a disaster. *Journal Of Business Continuity & Emergency Planning, 6*(4), 295 - 303. Retrieved September 12, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=3372a827-23d4-4136-8bfb-30b7687b1269%40sessionmgr4010

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017, September 1). User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach. *MIS Quarterly, 41*(3), 703 - 727. Retrieved January 8, 2018, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=7&sid=1ae81c32-17b1-4a71-a06d-158781fd8d15%40sessionmgr4007

Grant, R. M. (1988, June 12). On Dominant Logic, Relatedness and the Link Between Diversity and Performance. *Strategic Management Journal, 9*, 639 - 642. Retrieved November 14, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/detail/detail?vid=5&sid=63b0d5a8-85e4-4865-bf2e-1aba50ab9af6%40sessionmgr4008&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=12497023&db=bth

Grau, J. (2005, April 24). *Defining the Online Shopper*. Retrieved October 31, 2017, from Imedia Connection : http://www.imediaconnection.com/articles/ported-articles/red-dot-articles/2005/apr/defining-the-online-shopper/

Gupta, S. (2014, October 1). Cybercrime: Are Organisations Prepared Enough to Deal with it? *Human Capital*, 38 - 41. Retrieved October 14, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=9&sid=05a50e5e-b58c-4403-a859-adf09a373b58%40sessionmgr4008

Gyunka, B. A., & Christiana, A. O. (2017, May 1). Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. *Computing & Information Systems*, 10 - 18. Retrieved October 15, 2017, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=13&sid=aa3a4b76-29b0-4ddd-969f-4c18b3ce35bc%40sessionmgr103

Haesevoets, T., Hiel†, A. V., Pandelaere, M., Bostyn†, D. H., & Cremer, D. D. (2017, March). How much compensation is too much? An investigation of the effectiveness of financial overcompensation as a means to enhance customer loyalty. *Judgment and Decision Making, 12*(2), 183 - 197. Retrieved March 9, 2018, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=4&sid=8dce78ed-66a2-4ed4-a637-074bc7e70e2e%40sessionmgr103

Harvard Business Review. (2018, January 16). *For Better Customer Service, Offer Options, Not Apologies*. Retrieved March 1, 2018, from Harvard Business Review: https://hbr.org/ideacast/2018/01/for-better-customer-service-offer-options-not-apologies

Hewes Jr., C. A. (2016, March 1). Threat and Challenges of Cyber-Crime and. *SAM Advanced Management Journal*, 4 - 10. Retrieved September 8, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=d1033726-9da3-4bc0-9969-061dff4ad6af%40sessionmgr4008

Hilburg, A. (2013, November 15). *Why values matter in business: five key lessons from Tylenol Crisis from the "Tylenol Man" himself*. Retrieved November 3, 2017, from Biznews: https://www.biznews.com/thought-leaders/2013/11/15/five-key-lessons-from-tylenol-crisis/

Hsieha, M.-T., & Tsao, W.-C. (2014). Reducing perceived online shopping risk to enhance loyalty:a website quality perspective. *Journal of Risk Research, 17*(2), 241 - 261. Retrieved October 9, 2017, from http://0-

web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=7&sid=63b0d5a8-85e4-4865-bf2e-1aba50ab9af6%40sessionmgr4008

IT News Africa. (2017, March 7). *10 Biggest Cyber Crimes and Data Breaches*. Retrieved October 30, 2017, from IT News Africa: http://www.itnewsafrica.com/2017/03/10-biggest-cyber-crimes-and-data-breaches/

Julisch, K. (2013). Understanding and overcoming cybersecurity anti-patterns. *Computer Networks, 57*, 2206 - 2211. Retrieved October 29, 2017, from https://ac.els-cdn.com/S1389128613000388/1-s2.0-S1389128613000388-main.pdf?_tid=a3cef45a-b595-11e7-8a97-00000aacb362&acdnat=1508504176_e7e0c311023c2769093dc118a6bae13f

Kalof, L., Dan, A., & Dietz, T. (2008). *Essentials of Social Research.* New York: Open University Press.

Kellerman, B. (2006, April). *When Should a Leader Apologize, and When Not?* Retrieved March 1, 2018, from Harvard Business Review: https://hbr.org/2006/04/when-should-a-leader-apologize-and-when-not

Kohgadai, A. (2016, September 25). *The Right Way to Respond to a Data Breach*. Retrieved November 3, 2017, from Trip Wire: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-right-way-to-respond-to-a-data-breach/

Lee, H. (2016, October 1). The Role of Regulatory Focus in Online & Mobile Shopping focused on Shopping Motivations and Information Quality. *Proceedings of the Academy of Marketing Studies, 21*(2), 9 - 13. Retrieved March 5, 2018, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=22&sid=cb02e006-a84e-46e3-a3bf-d3ff5655c096%40sessionmgr4008

Lewis, E. (2002, August). Crisis, what crisis? *Brand Strategy*, 20 - 22. Retrieved December 22, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=10&sid=63b0d5a8-85e4-4865-bf2e-1aba50ab9af6%40sessionmgr4008

Lieberman, M. (2017, December 8). *Mind The Trust Gap: How Companies Can Retain Customers After A Security Breach*. Retrieved March 8, 2018, from Forbes: https://www.forbes.com/sites/forbestechcouncil/2017/12/08/mind-the-trust-gap-how-companies-can-retain-customers-after-a-security-breach/#4fbd57a26c95

Lord, N. (2017, July 27). *Data Breach Experts Share the Most Important Next Step You Should Take After a Data Breach in 2014 - 2015 & Beyond*. Retrieved November 3, 2017, from Digital Guardian: https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015

Lord, N. (2017, July 27). *The History of Data Breaches*. Retrieved October 25, 2017, from Digital Guardian : https://digitalguardian.com/blog/history-data-breaches

Lord, N. (2017, July 27). *What is Cyber Security?* Retrieved November 2, 2017, from Digital Guardian: https://digitalguardian.com/blog/what-cyber-security

Mahlaka, R. (2016, July 4). *Online shopping: Shifting purchasing realms*. Retrieved September 2017, 2017, from Moneyweb: https://www.moneyweb.co.za/in-depth/ecommerce/online-shopping-shifting-purchasing-realms/

Mallapragada, G., Chandukala, S. R., & Liu, Q. (2016, March). Exploring the Effects of "What" (Product) and "Where" (Website) Characteristics on Online Shopping Behavior. *Journal of Marketing, 80*, 21 - 38. Retrieved November 25, 2017, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=4&sid=5ae68470-a7e5-43fa-a2bf-714681c18494%40sessionmgr4010

McCoy, K. (2017, May 23). Target to pay $18.5M for 2013 data breach that affected 41 million consumers. *USA Today*, p. 1. Retrieved September 28, 2017, from https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

Mintzer, R. (2014, May 29). *Accepting Credit Cards and PayPal on Your eCommerce Site*. Retrieved November 1, 2017, from Entrepreneur Network: https://www.entrepreneur.com/article/234131

Moeller, S., Fassnacht, M., & Ettinger, A. (2009, October 1). Retaining Customers With Shopping Convenience. *Journal of Relationship Marketing, 8*, 313 - 329. Retrieved November 24, 2017, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=0603bb30-5492-4c6f-a703-ab22011d2f5b%40sessionmgr104

Morgan, S. (2017, October 18). *Top 5 cybersecurity facts, figures and statistics for 2017*. Retrieved October 24, 2017, from CSO: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Ogden, J. v. (2016, September 27). *Hacker vs. Disgruntled Employee vs. Human Error: Which is the Biggest Threat to Data Integrity?* Retrieved March 7, 2018, from CIMCOR: https://www.cimcor.com/blog/hacker-vs.-disgruntled-employee-vs.-human-error-which-is-the-biggest-threat-to-data-integrity

Olenski, S. (2016, August 3). *The Effect Of Cyber Crime On Online Shopping*. Retrieved March 5, 2018, from Forbes: https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/#1752da0c2b87

Panda, R., & Swar, B. N. (2013, October 1). Online Shopping: An Exploratory Study to Identify the Determinants of Shopper Buying Behaviour. *international Journal of Business Insights & Transformation, 7*, 52 - 59. Retrieved December 8, 2017, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=5&sid=04fd9962-e39c-4c9c-ac9a-6eceb03bd416%40sessionmgr101

Ragan, S. (2016, October 12). *Amazon resets customer passwords, while LeakedSource discloses massive update*. Retrieved January 9, 2018, from CSO: https://www.csoonline.com/article/3130298/security/amazon-resets-customer-passwords-while-leakedsource-discloses-massive-update.html

Rizkallah, J. (2017, July 11). *When A Data Breach Can Be A Benefit To Your Brand*. Retrieved October 30, 2017, from Forbes: https://www.forbes.com/sites/forbestechcouncil/2017/07/11/when-a-data-breach-can-be-a-benefit-to-your-brand/#68fc51404e6e

Roberts, P. (2017, January 26). *4,000 Data Breaches, 4 Billion Records: 2016 by the Numbers* . Retrieved October 24, 2017, from Digital Guardian : https://digitalguardian.com/blog/4000-breaches-4-billion-records-2016-numbers

Security Week News. (2016, February 25). *Over 700 Million Data Records Compromised in 2015: Report*. Retrieved October 25, 2017, from Security Week News: http://www.securityweek.com/over-700-million-data-records-compromised-2015-report

Sethi, U. J., & Sethi, R. S. (2016, October 1). Impact of Internet Usage Riskiness, Attitude towards Website Safety, Online Shopping Convenience on Online Purchase Intention. *International Journal of Research in Commerce & Management, 7*(10), 11 - 14. Retrieved March 5, 2018, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=14&sid=551b6209-6126-4193-b698-f4c74cfa0bb7%40sessionmgr4010

Shiue, Y.-C., & Li, L. S.-H. (2013, April 1). Brand Involvement in Retaining Customers Despite Dissatisfaction. *Social Behavior & Personality: an international journal, 41*(4), 643 - 650. Retrieved December 9, 2017, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=6&sid=d69b7cbe-a0d4-48ee-90fd-3612f5738505%40sessionmgr101

Skroupa, C. P. (2016, October 27). *Shareholders Sue Companies For Lying About Cyber Security*. Retrieved March 8, 2018, from Forbes: https://www.forbes.com/sites/christopherskroupa/2016/10/27/exposing-litigation-the-hidden-risks-of-cyber-breach/#3feda5af31a1

Smith, C. (2017, February 22). *SA e-commerce growing by leaps and bounds*. Retrieved September 30, 2017, from http://www.fin24.com/Companies/Retail/sa-e-commerce-growing-by-leaps-and-bounds-20170222

Spalević, Ž. (2014, January 2). Cyber Security As A Global Challenge Today. *Singidunum Journal of Applied Sciences*, 687 - 692. Retrieved September 30, 2017, from http://0-web.b.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=7&sid=aa3a4b76-29b0-4ddd-969f-4c18b3ce35bc%40sessionmgr103

Statista The Statistics Portal. (2017). *Retail e-commerce sales worldwide from 2014 to 2021*. Retrieved October 24, 2017, from Statista The Statistics Portal: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

Statista: The Statistics Portal. (2016). *Most popular devices for online shopping according to online shoppers worldwide in 2016, by region*. Retrieved October 31, 2017, from Statista: The Statistics Portal: https://www.statista.com/statistics/676407/preferred-device-for-online-shopping-by-region/

Tech Central. (2017, February 20). *Big growth in online shopping in SA*. Retrieved February 28, 20018, from Tech Central: https://techcentral.co.za/big-growth-in-online-shopping-in-sa/71943/

The Telegraph. (2017, August 14). *Cyber attacks on online retailers double in a year as hackers try to steal shoppers' details*. Retrieved September 30, 2017, from The Telegraph: http://www.telegraph.co.uk/news/2017/08/13/cyber-attacks-online-retailers-double-year-hackers-try-steal/

Tybout, A. M., & Roehm, M. (2009, December). *Let the Response Fit the Scandal*. Retrieved November 26, 2017, from Harvard Business Review: https://hbr.org/2009/12/let-the-response-fit-the-scandal

Vest, A. (2017, May 10). *Human Error and Cybersecurity: 4 Ways to Mitigate the Risk*. Retrieved October 25, 2017, from Huffington Post: https://www.huffingtonpost.com/entry/human-error-and-cybersecurity-4-ways-to-mitigate-the_us_590c8cd0e4b0f711807243c8

Vinton, K. (2014, July 1). *How Companies Can Rebuild Trust After A Security Breach*. Retrieved October 30, 2017, from Forbes: https://www.forbes.com/sites/katevinton/2014/07/01/how-companies-can-rebuild-trust-after-a-security-breach/#2a7eb9e75e6c

Whitler, K. A., & Farris, P. W. (2017, March 1). The Impact of Cyber Attacks On Brand Image Why Proactive Marketing Expertise Is Needed for Managing Data Breaches. *Journal of Advertising Research*, 3 - 9. Retrieved January 9, 2018, from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/pdfviewer/pdfviewer?vid=6&sid=95904de8-1ee2-41eb-837b-be35836503fc%40sessionmgr4008

Zadelhoff, M. v. (2016, September 19). *The Biggest Cybersecurity Threats Are Inside Your Company*. Retrieved October 30, 2017, from Harvard Business Review: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

Zyl, G. v. (2016, July 7). *8.8 million South Africans hit by cyber crime - study*. Retrieved September 29, 2017, from Fin 24: http://www.fin24.com/Tech/News/88-million-south-africans-hit-by-cyber-crime-study-20160707