Gordon Institute of Business Science
University of Pretoria

The impact of data breaches of varying severity on the customer loyalty of high net worth individuals in retail banking.

By

Senzosenkosi Nsibande

Student Number: 13094590

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

01 December 2020

Abstract

The aim of this study was to investigate the impact of data breaches of varying severity on customer loyalty. The study was motivated by the growth in the amount of data shared and stored by organisations to enhance service offerings (Big Data), and the increase in the frequency and scale of data breaches caused by this. Research shows that customer loyalty is critical to the long-term profitability of an organisation, making the understanding of data breaches on customer loyalty critical for any organisation's prospects. Despite this significance, literature on how breach severity can influence behavioural changes has been limited. This study, using an experiment, and the three dimensions of attribution theory - to assess how customers determine causal inference and assign blame following a breach - examined how customers changed their loyalty intentions following a data breach depending on the size and scale of the breach. This study aims to contribute to the existing body of work related to data breaches.

A 2X3 factorial design was used to determine the effects of the locus, the stability, and the controllability of cause on the customer's loyalty intentions, and to test the moderating effects of the breach severity. The results of the study determined that the stability and the controllability of cause were significant determinants of customer loyalty. The role of the severity and the locus of causality were determined to have limited bearing on customer loyalty. The implications for academia, managers and businesses are examined.

Keywords

Data breach, Data Privacy, Customer loyalty, Breach Severity, Attribution Theory

Declaration

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

Name: Senzosenkosi Nsibande

Signature: _____

Date: 01 December 2020

Contents

List of Tables

List of Figures

Chapter 1: Introduction to Research Problem

1.1. Research title

The study is entitled “The impact of data breaches of varying severity on the customer loyalty of high net worth individuals in retail banking”.

1.2. Introduction

In recent years, there has been a sharp increase in the frequency and scale of data breaches around the world (Martin & Murphy, 2017). This is in line with the data collected, stored, and used by companies to derive pure, actionable insights about their customers – Big data (Martin & Murphy, 2017). Access to this large quantum of data has subsequently necessitated more stringent data governance and controls to ensure customer personal information is not compromised through data breaches. According to Choi, Kim, and Jiang (2016), data breaches can occur due to a variety of reasons including employee negligence, phishing, malware, and software attacks, and vary in size and scale. This unauthorised access to sensitive company and/or customer information, depending on type and quantum, can lead to significant negative outcomes for the respective parties (Sen & Borle, 2015a).

For companies, the economic impact of data breaches can be high including reputational damage, loss in share value, loss of revenue, and general customer distrust. For example, the 2012 Sony data breach was estimated to have cost the company more than $171 million in related customer claims and lawsuits (Choi, Kim, & Jiang, 2016). Thus, understanding the impact of data breaches on customers has increased in importance.

Other, more recent data breach incidents include the 2018 Liberty data breach which resulted in millions of their client personal details being exposed, and the Financial Mail labelling the breach as “the biggest breach yet” (Shapshak, 2018, para. 1). In 2017, another reported compromise involved Jigsaw Holdings, a holding company for several real estate franchises (Fraser, 2017). The Jigsaw breach was reported to have occurred due to a misconfigured website with weak security and saw 60 million

records consisting of the personal data of South African citizens being compromised (Fraser, 2017). Data breaches, however, vary in size, type and impact and are not unique to South Africa. This was evident in 2015, where Target, a large American retailer, reported a data breach of approximately 100 million personal consumer credit card records (Choi et al., 2016).

Consumer interest regarding the way organisations store and use their sensitive data has also increased in recent years. This was evidenced by the outrage experienced following the recent scandal involving voter manipulation, where Cambridge Analytica used social media data obtained through Facebook to influence the United States presidential election (Lăzăroiu et al., 2018). Globally, countries have responded to consumer concerns by increasing data governance regulations and requirements for companies that collect, store and use sensitive customer data. Leading this enhanced regulation, has been the European Union, through the EU General Data Protection Regulation (GDPR), which is a comprehensive regulatory framework to govern themes like the transparency of data use, the manner of data storage and transition, and also regulates for mandatory data breach notifications to customers (Goddard, 2017). The United States also has a similar Act i.e. Privacy Act, which details how data breach notifications should be managed by organisations (Sen & Borle, 2015a). While the introduction of these privacy laws has been widely supported by consumers, their impact in reducing breaches and related crimes, like Identity Theft, are still being debated (Martin, Borah, & Palmatier, 2017). Despite ongoing debate, the need and implementation of these regulations exhibit the heightened public interest in understanding the impact of data breaches further.

According to Janakiraman, Lim, and Rishika (2018), due to the way in which information relating to data compromises is often shared, customers impacted by the compromise are likely to process the information more critically. This critical assessment is likely to result in a larger change in their behaviour, depending on the severity of the compromise, which can be against the company. Janakiraman, Lim, and Rishika (2018) further argue that a breach of customer information is a severe violation of the social contract which exists between a company and its consumers. Data breaches may, therefore, impact the relationship between the company and the consumer negatively, unless effectively managed. This, combined with the increased need to preserve the continued patronage of customers for the long-term profitability

of companies, necessitates the study to understand the impact of data breaches on customers loyalty (Ngobo, 2017).

By extending on the work by Janakiraman, Lim and Rishika (2018), in The Effect of a Data Breach Announcement on Customer Behaviour: Evidence from a Multichannel Retailer, who have highlighted the need to explore the role of breach severity as a factor when evaluating the impact of data breaches, this study sought to use attribution theory and its three dimensions of stability, locus of causality and controllability to establish the impact of data breach severity on the customer loyalty of clients.

1.3. Motivation for the Research Problem

This study focuses on the impact of data breaches on customer loyalty. The business and theoretical motivation for the study will be explored below:

A data breach is defined as the theft, loss, or compromise of personally identifiable information (Choi et al., 2016). In business, there has been sufficient research highlighting evidence that security breaches have an impact on a company's value/share price (Rosati, et al., 2017) (Kashmiri, Nicol, & Hsu, 2017) and reputation, with the breach severity aggravating negative sentiments towards the company (Martin et al., 2017). These impacts also extend to the customers of the breached organisation.

Literature in understanding the broader impacts of data breaches on the customer has been extensive. The existing research is focused on answering questions related to the negative impacts following a data breach announcement, how these impacts can be reduced through service recovery efforts (Choi et al., 2016) and how these translate into customer behaviour like purchase intention (Goode, Hoehle, Venkatesh, & Brown, 2017), engagement and switching (Martin et al., 2017). However, literature focused specifically on understanding the impact of the severity of a data breach on customer loyalty and retention has been limited (Janakiraman, Lim, & Rishika, 2018). Janakiraman et al (2018) observe that the larger the company, the greater the expectation on the company to protect customer information, and ultimately the greater the impact on a customer's negative perceptions to the brand

following a compromise. This can in turn impact the relationship between the company and the consumer negatively (Janakiraman et al., 2018). In addition, it is suggested that this requires further understanding to ensure customer loyalty can be maintained or improved during a data breach (Janakiraman, Lim, & Rishika, 2018).

In the Malhotra and Malhotra's (2011) study of customer information breaches as service failures, it is argued that data breaches can also be regarded as a service failure and a violation of the social contract by the company. They too, like Janakiraman et al (2018) observe that the larger the company, the greater the expectation on the company to protect customer information, and ultimately the greater the impact on a customer's negative perceptions (Malhotra & Malhotra, 2011).

With data breaches having the potential to significantly impact a business, the ability to understand them along with data privacy protection, can be used to derive competitive strategic advantages for companies (Martin et al., 2020). Marin et al. (2020) recently found that customers value privacy protection and would reward organisations that actively sought to manage this risk on their behalf. They show how data privacy is critical in generating a sustained competitive advantage. In addition, the level of transparency and controls over customer data exercised by companies has been established as a key driver of firm performance (Martin et al., 2017). Thus, as the type and rate of data collected increases, which may be unknown to consumers, companies need to understand the impacts of unsanctioned data use - which may lead to unwanted behaviours against the business (switching and negative word of mouth).

Furthermore, the expanse of personal identifiable information has increased in volume and type. This includes personal information, financial data and health data (Sen & Borle, 2015a). Sen and Borle (2015) state that the most severe impact of data breaches for individuals is identity theft, where personal data is used to defraud customers for large amounts of money annually. This provides some insight that the severity of the data breach may impact customers differently. While there are some initial pilot studies considering the role of severity on the impacts of data breaches(Aivazpour, Valecha, & Chakraborty, 2018), this remains an area of limited understanding. There is a need to understand how the number and type of records

compromised on a single breach can be used as a factor in influencing the type of strategy to deploy during a data breach in order to limit customer fallout. This, therefore, leaves a gap in the understanding and appreciation for businesses and academia.

For academics, understanding the manner in which customers infer the cause of an event like a data breach and their subsequent behavioural response, has been an area of interest for decades (Pick, Thomas, Tillmanns, & Krafft, 2016). While data breaches have remained topical for marketing studies, understanding how customers use their inference of cause to change behaviour has been limited. Attribution theory and its ability to analyse causal relationships has been identified as an appropriate lens to understand how customers respond (Weiner, 2001) through their loyalty intention, to a data breach. This is also used to understand how customers partition blame following a negative event (Song, Sheinin, & Yoon, 2016). This blame can extend to other negative outcomes, like changes in loyalty behaviours. This study sought to extend this body of knowledge by using attribution theory and its constructs in determining how customers assign blame during negative events – and how the negative event (in this instance – the breach event) leads to changes in their loyalty behaviour.

In addition, due to the frequency, scale and impact of data compromises on customer behaviour, it was important that academia further understand how these factors interacted during and after a data breach. This understanding will enhance the cognisance of influencers to customer decision-making. The insights from this study will also provide managers of data compromises with clearer areas of customer focus – ensuring that they deploy more relevant strategies and in turn also minimise any negative impacts on their customer bases. This study aims to (on the whole) add to the wider body of research on the effects of data breaches on customer behaviour even for other use cases not identified above.

In understanding the importance of customer loyalty, the study considers why it is valued by business and academia. Ngobo (2017) states that customers are loyal when they display a “preferential attitude” (p.229) towards an organisation. This can be displayed more deeply in the form of repeat patronage (DeWitt, Nguyen, & Marshall, 2008). There is evidence that suggests that customer loyalty is a trait that

is valued by organisations for numerous reasons, including that loyal customers attract new customers through positive sentiments shared about the organisation (Abratt & Russell, 1999; DeWitt et al., 2008; Ngobo, 2017).

Ngobo (2017) highlights that loyal customers also perform repeat purchases, thus improving the organisation's profitability over time (Chen, 2015). DeWitt, Nguyen and Marshall (2008) further affirm the importance of preserving customer loyalty for the long-term success of an organisation, especially during service recovery efforts. The value of customer loyalty to firms has also led to them incentivising loyal customers through their reward programmes, and utilising monetary compensation for failures like data breaches as a retentions mechanism (Goode et al., 2017). Thus, making loyalty a desired trait for many organisations to understand the drivers there of.

In addition, the ease in which negative sentiments (negative word of mouth) can be shared around data breaches, their perceived causes, and whether the breached organisation has the competency to manage any resultant customer harm, especially with the advent of social media, has meant that an organisations response to the breach has become critical in managing social sentiment for its reputation (Syed, 2019). Syed (2019) further extends this point, by stating that “28% of crisis information spreads globally within the first hour and failure to respond within the first 21 h leaves an organization open to “trial on Twitter””. (p.258). The above statement shows how data breaches and their perceived assessment and turnaround times strongly influence the reputation of an organisation, and customer behaviour and sentiment, like word of mouth. Being forthcoming and proactive in managing a data breach crisis is, therefore, important for the reputation of organisations. Based on the above, understanding the factors that adversely influence customer loyalty becomes critical for an organisation’s long-term success. This is especially true in the banking industry, where customer loyalty leads directly to increased profitability and reduced servicing costs (Sayani, 2015).

In substantiating the focus on high net worth clients; Banks have over the years been seen to have a keen interest in high net worth individuals, particularly those in private banking due to their impact on profitability and the segment’s overall growth rate (Abratt & Russell, 1999). Sayani (2015) also explains that high net worth individuals tend to have higher service expectations than individuals in lower-income groups

(Sayani, 2015) and may, therefore, be more sensitive to service failures such as data breaches. Critically, high net worth individuals also tend to hold relationships with multiple institutions simultaneously, resulting in reduced switching barriers when they are compared to other banking clients. It was previously determined that most banking clients are averse to switching brands due to the perceived high costs of switching and the reduced competition when compared to industries like retailing (Sayani, 2015). This means that the impact of data breaches on their loyalty may be more pronounced compared to that of regular banking clients.

To this end, banking institutions further enhanced the uniqueness of this study due to the quantum and variety of data collected and stored, compared to other institutions. This includes, but is not limited to, personal identifiable information (name, email, contact details, identity numbers, address, etc.), customer behaviour information (spending behaviour, credit behaviour, etc.) and financial data (credit card details, income, investments, etc.).

It is in this context that this study sought to find evidence that data breaches – depending on their severity - can influence customer behaviour, particularly their loyalty to the company. Therefore, the core objectives behind this study were: 1) to understand the factors that influence the change in desirable customer behaviour following a data breach and 2) determine the impact of the breach severity in influencing loyalty.

1.4. Purpose Statement

The purpose of this study was to utilise Attribution Theory to examine the extent to which the customer loyalty of high net worth banking clients was impacted by data breaches of varying severity. The study was performed through an experimental vignette design aiming to answer how data breach severities impact a client's behaviour, specifically customer loyalty.

This would be achieved by specifically looking at changes to customer loyalty within the banking industry, due to the elevated importance of sustained loyalty on the long-term profitability of companies in this industry. In line with similar studies, the

study controlled for variables including age, gender, previous breach experience and education (Aivazpour et al., 2018).

1.5. Research Objectives and Scope

1.5.1. Research Objective

The key research objectives for the study include:

Objective 1: To determine how the causal inference factors of Locus of causality, stability and controllability, influence customer loyalty following a data breach for high net worth clients in retail banking.

Objective 2: To understand the role of breach severity in influencing the relationship between the factors identified in objective one, and the customer loyalty of high net worth clients, by presenting six different breach scenarios controlled for breach severity. Do customers respond differently to data breaches of varying severity?

1.5.2. Research Scope

The primary aim of the research is to understand the impact of data breach severity on the customer loyalty of high net worth retail banking clients. The geographic scope of the research is retail and private banking in South Africa, specifically for individuals above the age of 18 years.

1.6. Conclusion and Report Structure

In the first chapter, an argument was made for the need for this study - for both business and academia alike. This was achieved by presenting the background on past data breaches, their impact on customer loyalty and considering the less explored role of breach severity in influencing these factors. Focusing on retail banking and on specifically high net worth clients is expected to increase the uniqueness of the study. The banking industry is a sector with large amounts of

sensitive data, where the impacts of breaches can have a significant impact on overall profitability.

The remainder of the research report is organised as follows:

- Chapter two provides a literature review of the topic, providing further evidence for why this study is needed. This then culminates in hypotheses and research questions considered in the study.

- Chapter three finalises the statistical hypothesis guiding this study i.e. the hypothesis as set out in Chapter two. Chapter four aims to discuss and defend the chosen methodology for the study.

- The results collected in the study are presented in chapter five. This is then followed by a critical evaluation of the results in Chapter six, where key insights and findings are highlighted. These chapters will be aligned to the objectives presented in chapter one, and the hypothesis outlined in chapter two.

- Chapter seven concludes the report – providing the principal findings, limitations and recommendations for future research.

Chapter 2: Literature Review

2.1. Introduction

This chapter reviews the relevant academic literature related to data breaches, attribution theory, breach severity, customer loyalty and other key topics as they may relate to the study. Also, the chapter corroborates the need for the research topic as presented in Chapter one.

The chapter will begin with a brief background of data privacy and what previous studies have found to be the impact of data breaches on the relationship between customers and organisations. We then proceed to use Attribution Theory and its key dimensions to derive hypotheses for the factors that influence customer loyalty post a data breach, before considering the moderating role of data breach severity. A theoretical overview of customer loyalty as a concept is then provided focusing on its core constructs, namely word of mouth, repeat patronage, and most significantly, switching behaviour which is discussed in detail. Finally, these components culminate into the proposed research model which forms part of the conclusion that ending this chapter.

2.2. Data breaches

In this section, the study firstly considers data breaches as privacy breaches. It then uses privacy literature to define breaches and considers their impact on business and customers. The study goes on to using Marketing and Consumer Research literature to further unpack the impacts of data breaches by considering them as service failures, showing how companies that have been entrusted to safely store and use sensitive customer data have violated the psychological contract between the buyer of the service, and the seller of the service. The study concludes the section by introducing the academic lens of Attribution theory guiding the study.

2.2.1. Privacy Breaches

Privacy literature defines a data breach as the electronic theft, loss or compromise of personal identifiable information by parties external to the organisation (Choi et

al., 2016) (Goode et al., 2017). Marketing has approached the topic of data breaches with differing lenses, either related to the impacts of breaches on the customer (Goode et al., 2017; Janakiraman et al., 2018), the firm (Martin et al., 2017; Pick & Eisend, 2014) or the industry the firm operates in (Kashmiri et al., 2017). However, the broad consensus is that data breaches have a negative impact on both organisations and customers.

According to Casadesus-Masanell and Hervas-Drane (2015), firms collect large amounts of data to customise offerings to customers through differentiated products, servicing and advertising in a form of information exploitation. Customers trade-off the rewards of the increased utility of the service compared to the risk of the negative impacts of privacy breaches when sharing personal information for firms to exploit. Using theoretical models, they found that firms can benefit from differentiating their privacy policies and splitting customers based on their willingness to disclose information (Casadesus-Masanell & Hervas-Drane, 2015). Furthermore, it was determined that the management of data privacy is highly valued by clients, and can be used to derive a competitive advantage for organisations (Martin et al., 2020).

For organisations, the negative impacts of data breaches on performance have been sufficiently researched in recent years in line with the growth of data storage and usage (Choi et al., 2016; Kashmiri et al., 2017). The consequences of a firm announcing a data breach can be vast, including increased future acquisition costs and the loss of existing customers (Janakiraman et al., 2018). Most research papers focus on the negative impacts on the firm at a macro-level (Aivazpour et al., 2018), like changes in share price (Kashmiri et al., 2017), changes in channel usage (Choi et al., 2016) or the loss in brand equity and reputation. These impacts vary according to the size, industry and the goods and services a firm provides (Martin et al., 2017).

In line with the growing volume of customer data collected and shared with organisations, privacy literature has also found that there is an increased expectation by customers for organisations to protect this data in line with data privacy regulations (Martin & Murphy, 2017). In addition, when sharing data, consumers enter a social contract with the organisation and seek to obtain a fair return on this agreement through enhanced offerings and the appropriate use of their data. Therefore, if the data is breached and used unjustly, it is viewed by the consumer as

a violation of the said social contract (Malhotra & Malhotra, 2011). A data breach is therefore viewed as a contravention of this psychological contract that has been established between themselves and the impacted organisation to safeguard their data and prevent potential future harm (Goode et al., 2017). In addition, customers who have shared their data willingly tend to experience feelings of vulnerability and violation and will look to protect themselves against future harm unless the trust relationship is timeously restored (Choi et al., 2016).

Once customers have experienced a data breach, their attitude towards an organisation may change, and this change may be in the form of negative word of mouth or even falsifying information about the organisation (Martin et al., 2017), both are traits of diminishing customer loyalty. This has led to a new branch of service recovery research focusing on determining factors that can be used to restore the trust and maintain customer loyalty during a data breach (Choi et al., 2016; Goode et al., 2017). Using justice theories, they state that a customer will evaluate recovery efforts as just or unjust based on the tangible outcomes (distributive justice), the process (procedural justice) and the way they are treated (interactional justice) during these recovery efforts (DeWitt et al., 2008; Goode et al., 2017).

2.2.2. Data breaches as Service failures

While data breaches can be viewed as system and privacy failures, they can also be assessed as service failures, especially when the storage and safeguarding of data is viewed as part of the service offering of the company providing the service (Malhotra & Malhotra, 2011). Some breaches can also lead to direct harm to the customer in the form of identity theft, with service research further accounting for them under product-harm crisis – direct harm from the product or service failure (Munyon, Jenkins, Crook, Edwards, & Harvey, 2019).

When considering data breaches and their impact at two levels, the organisation (or brand) and the customer, the following was determined.

According to Wan, Hui, Wyer (2011), service encounters are exchange relationships that tend to be impersonal and transactional in nature. That is, there is an expectation that one benefit is traded for a perceived equivalent benefit in the form of service.

Alternatively, some can be viewed as communal or friendships relationships with the service provider. By studying the customer responses to service failures in exchange relationships when compared to communal (friendship) relationships, they found that in both instances' customers interpreted the service failure as a breach in obligations by the service provider (Wan, Hui, & Wyer, 2011). Those that viewed the relationship as simply an exchange relationship treated the service failure as another type contract breach, while customers who had more of a communal relationship with the service provider, experienced further feelings of betrayal where the friendship did not negate negative reactions to the service failure (Wan et al., 2011). This means, data breaches seen as an extension of service failures will negatively influence all customers despite the perceived nature of the relationship with the organisation, and more importantly, this may vary in severity.

Further research considering data breaches as a product harm crisis also support this view and have found that customers will seek to attribute blame to those responsible for causing the crisis through changes in their customer behaviour (Whelan & Dawar, 2016). This is in line with the findings of studies which consider data breaches as service failures, where data protection forms part of the service provided by the organisations (Janakiraman et al., 2018). Recent literature has also found that some customers who are more loyal to organisations, respond more severely to product failures, driven by feelings of betrayal (Cleeren, Dekimpe, & Heerde, 2017). They further note, that the response to service failures, like data breaches, is worsened by increased media attention and the severity of the product failure (Cleeren et al., 2017).

According to Whelan and Dawar (2016), it was found that the attribution of blame for a service failure, like data breaches, acts as a mediator between the consequences of the data breach and the appraisal of the brand. Furthermore, Puzakova, Kwak and Rocereto (2013) determined that the brand position of the organisation also influences the way customers respond to negative news like data breaches. They found that customers responded worse to negative publicity for anthropomorphized (humanised) brands than those that were non-anthropomorphized (non-humanised). This stemmed from the tendency for people to associate the wrongdoings of someone as being caused by the inherent factors of the transgressor, and not environmental or situational factors (Puzakova, Kwak, & Rocereto, 2013). This view

then extends to transgressing companies that are viewed as human-like, where customers assess them as having caused the negative outcome and having a higher likelihood of perpetrating the wrongdoing in future. This is due to the cause being assumed to be inherent to the organisation's nature. This assessment then determined the extent to which consumers chose to punish the organisation for the transgression.

Using implicit theory they also determined that customers that believed personality traits were fixed (incremental theorists) and consistent, responded more negatively to negative news than those customers who viewed personality traits as malleable or varying (implicit theorists) (Puzakova et al., 2013). This research highlights that data breaches 1) may be attributed to the breached organisation, then other factors. 2) the breach may have varying impacts on customers depending on brand perception and how customers attribute humanlike characteristics (like personality and human nature) to the brand i.e. bad people do bad things. 3) the severity in response against the organisation due to the breach may be varied based on the customer's attribution of blame.

Hui Liao (2007), in his study of service recovery on customer loyalty, explained that disappointed customers share their bad experience with between ten and twenty individuals after a service failure. This distribution of negative sentiments can impact the brand of an organisation adversely. The study also found that service recovery attempts by organisations following a service failure were likely to be successful if the organisation explained the reasons for the service failure. Lastly, they determined that the severity of the failure had a moderating role in service recovery efforts and customer satisfaction (Liao, 2007). That is, customers will respond to service failures, like data breaches differently depending on the recovery efforts of the company. These responses may, however, vary depending on the severity and extent of the service failure.

In line with service failure research, understanding the cause of a failure, the way customers attribute blame and their subsequent behavioural responses– attribution theory has often been viewed as most appropriate in this assessment (Munyon et

al., 2019; Pick et al., 2016). We now use attribution theory to further explore the impact of data breaches on customer loyalty.

2.3. Attribution Theory

Thus far, it has been determined that data breaches can have varying negative impacts on customers and companies alike. This variation is driven by the customers' perceptions regarding the role of the organisation has played in protecting their personal information. Furthermore, inferences related to whether the breach could have been prevented are also important elements for determining blame. The study employs attribution theory to determine customer perceptions regarding the causes of the breach, and how these will influence their subsequent behaviour towards the organisation.

Attribution theory assumes individuals process information rationally and subsequently infer the cause of events to influence their attitude or behaviour (Pick et al., 2016). This can be used to understand loyalty attributes and behaviours following a data breach. The theory suggests that perceived causes of success or failure are grouped into three main dimensions, namely; locus, stability and controllability, which will, in turn, drive customer behaviour (Pick et al., 2016).

There is a requirement by both customers and organisations to understand the underlying causes of success and failure - to influence and limit the likelihood of an undesired outcome like economic loss, product failure, rejection or otherwise (Weiner, 1985). Data breaches can be considered as one of these service failures (Choi et al., 2016). Attribution Theory has been useful in executing these causal assessments, especially in consumer research. It has also been widely used to explain how blame is placed following negative events or crises - including service and product failures (Munyon et al., 2019). Weiner (2001), explains that the purchase of products and services can result in both positive and negative outcomes and that it is logical to reason that consumers will attribute this success or failure to an underlying cause, which will then influence subsequent consumer behaviour for or against this outcome. This can be in the form of repeat purchases or conversely, changing a supplier.

The study introduces the three dimensions of Attribution theory and utilises them to derive hypotheses for factors that influence customer loyalty following a data breach of a customer's personal identifiable information.

2.3.1. Locus of Causality

The Locus of causality refers to whether a customer views the cause of an outcome as being driven by an internal or external factor (Munyon et al., 2019). The key question in establishing this is whether the customer views the failure as being directly related to a factor that is within their control (internal locus), or due to an external factor including the company providing the product or service (external locus)(Pick et al., 2016). It can also be articulated as the perception by a customer, of who is responsible for the failure (Huang, 2008).

Customers will associate responsibility for negative news based on who they view as being responsible for the breach (Munyon et al., 2019). Munyon et al (2019) further state that the determination of judgement requires that there be a clear locus of causality, followed by a level of controllability, which will be discussed in the next subsection. Pick, Thomas, Tillmanns and Krafft (2016) further state that customers that associate the failure directly with the company providing the service (external locus), are likely to display lower loyalty and willingness to repurchase from that company. Customers also tend to associate positive outcomes due to their own actions and negative outcomes due to the actions of others (hedonic bias)(Weiner, 1985). Based on this, it is expected that customers will associate the negative impacts of a data breach as being due to an external factor over one that is internal.

In line with the attributional process of determining the responsibility of negative news, Martin and Murphy (2017) state that during the sharing of information, customers also shift responsibility for data protection to the organisation (privacy protection). The subsequent failure by an organisation to fulfil these expectations and obligations related to data privacy through a data breach can be seen as a breach of the psychological contract which exists between the organisation and its customers (Goode et al., 2017). This perceived breach in the psychological contract by the organisation (external locus) leads to reduced commitment and reduced future

purchase intentions towards the organisation by the customer (Goode et al., 2017). They provide research that shows that 40% of surveyed customers state that they would consider discontinuing the relationship with a company that had been breached, citing unfulfilled service quality expectations. This supports the views that data breaches can be considered service failures, and form part of service failure research.

Malhotra and Malhotra's (2011) study of customer information breaches as service failures, is also extensively cited (Martin & Murphy, 2017)(Choi et al., 2016)(Kashmiri et al., 2017) as confirmation that the breach in customer information can indeed be considered by customers as a service failure attributed to the organisation's actions (external locus). Once customers have determined the breach as a service failure, and by extension an outcome caused by an external factor (locus), it will influence customer behaviour including word of mouth and future switching intention(Choi et al., 2016).

Based on this reasoning, we expected that an increased perceived external locus of causality by customers would negatively influence customer loyalty and presented the first hypothesis below:

H1: The more customers infer the cause of the data breach as being directly caused by an organisation (external locus), the lower their loyalty to that organisation.

Once customers have determined the locus of causality, they will then investigate the stability and control dimensions in order to determine judgement and subsequent response (Munyon et al., 2019). Next, consider the dimension related to stability.

2.3.2. Stability of Cause

The perceived stability of the cause, and whether the failure is stable or unstable, will influence customer behaviour (Pick et al., 2016). Customers who perceive a data breach as having a high likelihood of reoccurring in the future (stable), will have a low likelihood of repeat purchase behaviour in the future (Goode et al., 2017). Further, there is literature, borrowed from the concept of psychological response evaluation, that claims that a breach of customer information can increase a

customers' perceived view of further harm in the future (Choi et al., 2016), and the impacted company may therefore need to take necessary precautions to manage this perceived loss (Mikhed & Vogan, 2018). These precautionary measures may be against the desired outcomes of a company, for example, buying less or closing off their account.

For retailers announcing data breaches, perceptions of broad vulnerabilities may lead to negative impacts on sales channels that are not compromised (spill over), due to the fear by customers of the compromise reoccurring through other channels (Janakiraman et al., 2018). This perceived recurrence of the negative outcome can result in adverse purchasing behaviour against a breached organisation.

In a study using attachment theory, which is derived by determining a view of self (anxiety) and a view of others (avoidance), to evaluate the manner in which blame is placed post an unexpected product crisis, the research found that the two of the four attachment styles (secure attachment and fearful attachment) that reflected the strongest brand affinity would attribute the least amount of blame to the organisation (Whelan & Dawar, 2016). That is, those that trusted the brand or feared consequences of going against the brand i.e. depicted low anxiety, low avoidance (secure attachment) and high anxiety, high avoidance (fearful attachment), would apportion the least amount of blame the organisation. However, they found that even these styles would only consider the negative news only once as a once-off event, and would shift blame should it reoccur or have a high likelihood of reoccurrence (Whelan & Dawar, 2016).

Based on this, it is hypothesised that:

H2: The more customers perceive the conditions of the breaches as stable (highly likely to recur), the less likely they are to remain loyal to that organisation.

2.3.3. Controllability of Cause

The last dimension of the Attribution theory evaluates the perceived control of an underlying cause that an individual attributes to a negative outcome, like a data breach (Pick et al., 2016). This refers to the customer's belief as to whether the

organisation could have prevented the failure (Huang, 2008). Specifically, upon a data breach, a customer's interpretation of the level of control an organisation has for preventing the data breach may influence the customer behaviour (Munyon et al., 2019).

Skinner (1996) defines control as "the extent to which an agent can intentionally produce desired outcomes and prevent undesired ones" (p.552). She further states that when evaluating control two outcomes must be met. An individual or organisation must have 1) effective means and 2) access to those means, to create the desired outcome (Skinner, 1996).

Senior managers of breached organisations are blamed post data breaches for not appropriately managing the data privacy duties of the organisation – both by investors and customers alike (Kashmiri et al., 2017). These perceptions of negligence may result in broad judgement for the impacted organisation, and other firms of similar size and industry, due to the effects explained by Associative network theory (Kashmiri et al., 2017). This theory explains how customers transfer the perceived causes of negative events, onto firms of similar size or industry i.e. If a company is breached and customers believe it was caused by lax privacy controls, they will then assume firms of similar size within the industry also have the same lax controls.

However, Martin and Murphey (2017) state that enabling customers to have more control over their data usage and security can suppress perceptions of vulnerabilities and limit the negative impacts of a data breach as control, and by extension responsibility, is shared across the organisation and the customer. They also state that increasing perceived control of consumer data builds the trust between the customer and the organisation (Martin & Murphy, 2017). Customers are more likely to share sensitive information with an organisation they can trust. Increasing perceived control of customer data builds the trust between the customer and the organisation.

In addition, when considering control as a construct, it is often subjective more than objective. According to Skinner (1996), an individual's perceived control will influence their behaviour independent of the objective control available to the individual. The

higher the perceived control the more likely an individual is to take initiative and responsibility for negative outcomes(self-blame). In instances where perceived control is low, a higher reliance is placed on those with authority or superior control (i.e. doctors treating frail patients), resulting in emotions of disappointment and blame, should negative impacts arise that are perceived to be in the control of others.

Monroe and Lane (2019) also argue that theories related to blame, collectively referred to as the motivated-blame models, also suggest that individuals pass judgement upfront post a negative event like a data breach, then later factor controllability as a key element to rationalise their judgement when determining blame. Furthermore, controllability is often exaggerated to justify the blame placed on the infringing party. However, their study found that blame is significantly reduced if it is considered unintended and unpreventable (Monroe & Lane, 2019). The third hypothesis:

H3: The more customers perceive the cause of the breach to be under their own control, the more willing the customer is to remain loyal to the organisation.

In summary, we use Attribution theory to explain how customers will determine the cause of negative events including data breaches and subsequently shift loyalty behaviour, by exploring the three dimensions of the theory, namely; locus of causality, stability and the level of perceived control they have over preventing negative outcomes. This has been determined to be a suitable theoretical framework for the study.

2.4. Data Breach Severity

The Study now considers the role of severity as a moderator in influencing customer loyalty and the dimensions of attribution theory. Severity is defined as “the magnitude of loss that is experienced by the customer due to an adverse incident” (Huang, 2008, pp. 525-1). For customers, the most severe data breach is one that leads to identity theft, which results in significant financial losses for customers (Sen & Borle, 2015a). Aivazpour et al (2018) also state that customers value the different types of personal identifiable information differently based on the perceived risk they pose.

Research has seldomly considered the role of data breach severity as a factor in explaining behavioural changes, especially at an individual customer level (micro level). Aivazpour, Valecha, Chakraborty (2018), state that information is not valued the same by all customers. Additionally - the type, amount and manner in which information was stolen may lead to varying levels of impact on customers (Aivazpour et al., 2018). Furthermore, Malhotra and Malhotra (2011), in their early research of data breaches as service failures, also found that large companies were impacted differently depending on the magnitude of a data breach. Their results showed that the larger company and magnitude of the breach, the higher the perception that the company could have prevented it. This provides evidence that customers will respond differently based on the different types of personal identifiable information that is compromised.

When considering data breaches as product failures, some failures may have low impacts, while others may result in larger consequences for customers (Song et al., 2016). Song, Sheinin and Yoon (2016) further state that the higher the consequences of the failure for a customer, the larger the need to understand the perceived reason for the failure in order to mitigate future occurrence is, in line with Attribution theory. Using Defensive Attribution Theory, a concept from psychology, it is also argued that the more severe the negative outcome, the stronger the need to attribute responsibility to the cause of the outcome (external locus of causality) (Zhou & Ki, 2018). This highlights that severity may influence the relationship between the perceived cause of an outcome (attribution theory) and the subsequent change in customer behaviour to protect against the adverse event in future (i.e. change in customer loyalty).

There is also research at a company-level that supports the view that data breach severity impacts the stock prices of organisations differently (Martin & Murphy, 2017). However, to our knowledge, research on the specific impacts of data breaches and their severity on individual customers has been limited. In addition, previous studies involving severity have focused on severity as driven by the outcome i.e. whether the outcome can result in direct harm, and have not considered factors like type and source of a breach, which will be considered widely in this study. This enunciates the uniqueness of this study as it aims to consider the role of severity (type and volume) in assessing the impact of data breaches on customer loyalty.

Further to this, Aivazpour, Valecha, Chakraborty (2018), in their short study state that the severity of data breaches is dependent on a combination of weighted values that consider three core elements: the types of records compromised (financial, account access, identity, nuanced, existential) the source of the breach and lastly whether the data can be used to cause harm to individuals. They use a combination of these factors to define severity as low, moderate or high (Aivazpour et al., 2018).

In addition, Stiennon (2013) reiterates the need for a holistic measure for the severity of data breaches and provides a Data Breach Index which identifies these three factors as most relevant in categorising data breach severities (Stiennon, 2013). While there may be additional influences to the other two dimensions of Attribution theory (stability and controllability), we expect that the higher the perceived data breach severity, the more likely the customer will direct blame towards the organisation (external locus) over self. This is expected to result in adverse changes in the customer's loyalty towards the firm. Thus, it is hypothesised that:

H4: Data breach severity negatively influences the relationship between perceived locus of causality and customer loyalty.

2.5. Customer Loyalty

Customer loyalty is defined as "the strength of the relationship between an individual's relative attitude and repeat patronage" (Dick & Basu, 1994, pp. 99-1). Customer loyalty can be classified into three varying classifications: no loyalty, latent loyalty and true loyalty, which can change over time based on customer age and information supplied (Ngobo, 2017). Latent loyalty (attitudinal loyalty) is a psychological loyalty which results in moderate loyalty behaviours like repeat purchase when convenient (Wolter, Bock, Smith, & Cronin, 2017). In comparison, true loyalty (conative loyalty) results in loyalty behaviours like repeat patronage and unsolicited word of mouth promotion of an organisation, despite the presence of barriers (Wolter et al., 2017), in our case, data breaches implicating an organisation. This true Loyalty can also be evidenced by a higher share of wallet and inconvenient patronage even post an adverse event like a data breach, and when it is inconvenient for consumers (Ngobo, 2017; Wolter et al., 2017). Customer loyalty is also closely

linked to the profitability of an organisation, increasing its relevance in consumer research (Ngobo, 2017). Ngobo (2017) states that the profitability of truly loyal customers is derived from the repeated purchases made by these customers.

Previous studies on the negative impacts on customer loyalty have used the negativity effect to explain that, customers who previously had a positive involvement with a company or brand, will have a more subdued response to negative news - like a data compromise (Ahluwalia, 2002). This is more pronounced when compared to customers who have no positive or subdued attitude to the brand who seemingly have a disproportionately high weighting to negative news regarding a brand or company (Ahluwalia, 2002). This is further illustrated in the study by Janakiraman, Lim and Rishika (2018) on the negative effects of data breach announcements on consumers, where they determined that the negative impact of data breach announcements on customers with low patronage is high. This supports the idea that customers do not respond homogenously to data breaches (Janakiraman et al., 2018). Research explains that companies should understand their customer loyalty intrinsically to apply appropriate strategies and to retain their customer base with appropriate initiatives (Ngobo, 2017).

2.5.1. Switching Behaviour Intention and Switching Costs

The most severe adverse response to customer loyalty outside of negative word of mouth and reduced patronage is switching behaviour (Watson, Beck, Henderson, & Palmatier, 2015). Switching behaviour refers to the replacement or change of a product, service or supplier to an alternative, and would be considered the direct opposite of customer loyalty (Jung, Han, & Oh, 2017). Switching away from a supplier is undesirable to the organisation due to its negative impacts on profitability. It also limits other loyalty traits of repeat purchase and positive word of mouth.

The Push-Pull Model has been used to explain and derive factors for customer switching behaviour. The Push-Pull Model is derived from migration theory and used to understand the factors that cause customers to move from one place to another (switch), they determined that pull factors where more positive factors which made the new destination more attractive. While push factors were more negative in nature and gave reasons why people should leave based on their current destination. Jung,

Han and Oh (2017) further cite that push factors are intricately linked to service quality and satisfaction. Furthermore, when service quality is not maintained, characterised by service failure, this can lead to switching behaviour (Jung et al., 2017).

Previous literature had considered data breaches as service failure, and when extending this to the PPM model, we then consider a data breach as a push factor that may result in customers switching their supplier for an alternative to prevent future harm post a data breach. Choi, Kim and Jiang (2016), state that organisations should take necessary steps to guard against switching behaviour as customer loyalty can be simply lost.

However, the likelihood of switching behaviours for customers is somewhat reduced depending on the perceived switching costs. These vary depending on the perceived ease (perceived effort, monetary or phycological) of replacing the product or service (Dick & Basu, 1994). Porter (2008), defined switching costs as fixed costs facing the buyer incurs for switching from one supplier's product to another. These costs can be as a result of the available alternatives in the market, product features (innovation and technology), number of suitable suppliers, or financial in nature (Porter, 2008).

As discussed, research suggests that loyalty is linked to attitudes and purchase behaviours (Watson et al., 2015). According to Watson, Beck, Henderson and Palmateir (2015), strong positive attitude towards a supplier limit switching behaviours with positive previous experiences further increasing switching costs. Earlier studies also found that the higher the perceived switching costs the more loyal the customer was likely to be (Ping, 1993). Pick and Eisend (2014), support the view and extend it by arguing that previous experiences increase emotional switching barriers for customers, however, they argue that these positive attitudes will be assessed critically against negative incidents like data breaches, which are well known to be drivers of switching behaviours, due to anger being a strong motivator for switching. Furthermore, they found that customers have a lower tolerance for negative service events (service failures) than for other switching causes like better competitor offerings and relational costs.

2.5.2. Switching Behaviour in explaining the customer loyalty of High Net worth Individuals (HNI's)

Following on from the literature, the switching behaviour intention of customers is a critical component in explaining the customer loyalty and is highly influenced by the perceived switching costs associated with the change (Blut, Frennea, Mittal, & Mothersbaugh, 2015). Switching costs include a combination of financial, time, psychological, relational and ability to switch (Blut et al., 2015). This ability to switch and the high perceived financial costs associated with a switch, means switching is better enabled for those who have the financial and ability to switch (Pick & Eisend, 2014). This study explores this population by terming it high net-worth– who have the financial means to switch suppliers. This definition of high net worth will be further refined in chapter four as adapted for the study. Sayani (2015) also states that these clients have a stronger ability to switch as they tend to have access to multiple suppliers even in industries like banking where switching barriers are significantly higher.

According to Pick and Eisend (2014), in their study of perceived switching costs and their impact on switching behaviour, they found that non-monetary reasons for switching rank higher than monetary reasons, except in the instance where the switching behaviour intention is as a result of a negative event. That is, in the instance of a negative event like a data breach, customers would consider mainly the financial impacts of switching, with those with the means initiate the switch more likely to finalise it. Thus, to sufficiently understand the impacts in customer loyalty of customers, especially in banking, switching and the barriers limiting it would have to be addressed in the study.

Furthermore, according to Beerli, Martin and Quintana (2004), the length of relationship and familiarity of banking staff also contributes significantly to sustained positive loyalty intention acting as a psychological switching barrier for customers with long standing relationships with the institution. This is said to be true even in the midst of dissatisfaction (Beerli, Martin, & Quintana, 2004)

This understanding of the constructs related to customer loyalty was used to investigate the impact of data breaches of varying severity. Moreover, while in this

study switching behaviour performs only as a single component in the broader construct of evaluating customer loyalty, it has been discussed in the literature due to its significance within the constructs of customer loyalty compared to others like repeat patronage and negative word of mouth.

2.6. Conclusion

The research aims to contribute to the wider body of literature related to data breaches and their effects on customer loyalty. The literature showed how Attribution theory can be used to explain the causal effects of changing customer behaviour post a data breach. Using constructs and dimensions provided by attribution theory, the study will investigate the locus of causality, the stability of the cause and the perceived level of control to understand these behaviour changes, if any, after a data breach announcement.

The literature review has also highlighted that customer loyalty and the changes thereof, is a key behavioural change, that is undergone by customers post a data breach and may be adversely influenced as a result of the breach. Organisations have a strong incentive to maintain the loyalty of their customers, especially post negative news like data breach announcements, due to its importance to long-term organisational sustainability and profitability (Chen, 2015). The literature also shown that the worst of these changes in customer loyalty is the switching of customers to another supplier of the service. This switching behaviour can be subdued depending on the strength of the switching barriers established. However, negative events like data breaches are expected to significantly increase switching behaviours due to the feelings of violation felt by customers of the breach organisation. However, switching in the study will be evaluated along with the other constructs of customer loyalty of repeat patronage and word of mouth, and the study intended to capture broad components of customer loyally under a single measure.

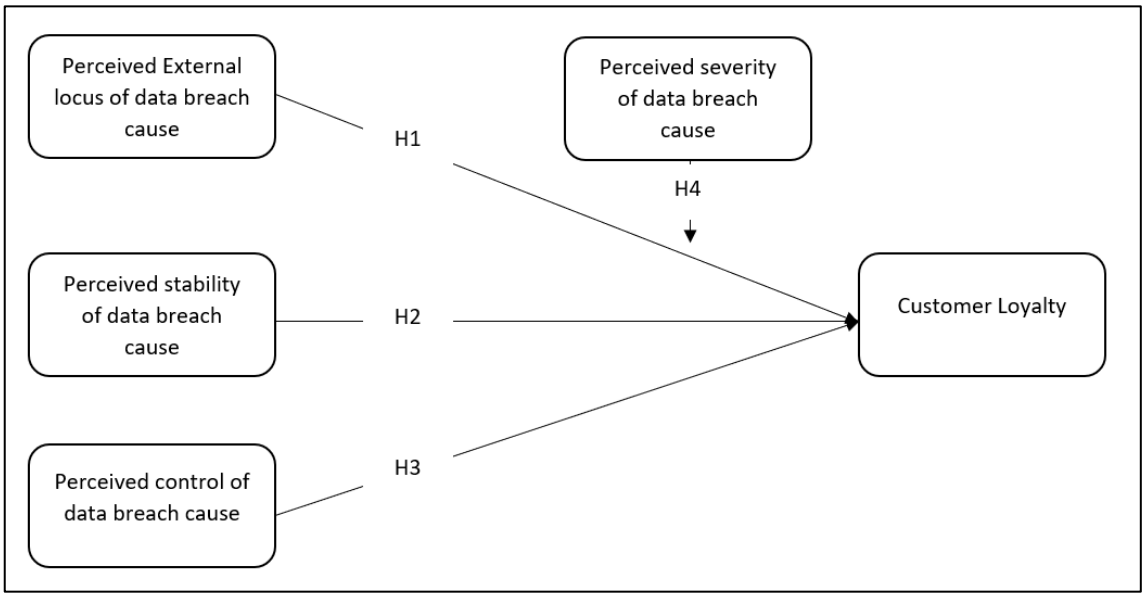
Lastly, the role of the breach severity, especially on customer loyalty, is one that literature has not sufficiently explored. This study aims to enrich the literature by establishing the severity of a breach as a moderator for the effects of data breaches on customer loyalty – particularly related to the type, volume and perceived impacts of a breach.

This moderating effect will give insights on how customers respond when breached information varies in volume and type, critical for academics, business and those managing the impacts of the breach when developing strategies to manage the effects.

We conclude this chapter by presenting a simplified research model summarising the hypothesis that we will be explored in the study. This will be further stated in Chapter three.

Based on the four hypothesised outcomes we propose the following research model:

Figure 1: Research Model



Chapter 3: Research Hypothesis

The literature review in the previous chapter highlighted that customers infer the perceived cause of negative events like data breaches to determine their subsequent behaviour (Pick et al., 2016). Attribution theory was then identified as an appropriate lens for the study to explore the impacts of data breach events and their subsequent effect on customer loyalty. Focus was given to the three dimensions of the theory, namely locus of causality, stability of cause and controllability of cause.

In addition, the literature review highlighted that the impacts of customer loyalty post the breach can differ depending on the severity (type, size and impact) of the breached data. Severity may then play a moderating role between the cause of data breaches and their impact on customer loyalty.

In order to explore the impacts of data breaches on customer loyalty and understand the moderating role of breach severity, the research objectives of the study are combined with the literature review to determine the research hypothesis that will guide the study.

3.1. Locus of Causality

The literature review in the previous chapter explained that the first dimension of attribution theory related to the locus of causality – is the outcome-driven by an internal or external factor. It was argued that in the instance of data breaches, it was expected that an increased perceived external locus of causality by customers would negatively influence customer loyalty. The null hypothesis states that a perceived external locus of causality (ELC) of the data breach will not have an impact on customer loyalty (CL). The alternative hypothesis states that a perceived external locus of causality of the data breach will negatively impact on customer loyalty (CL).

$H1_0$: $CL_{ELC} – CL=0$
$H1_1$: $CL_{ELC} – CL >0$

3.2. Stability of Cause

The literature reviewed in the previous chapter also argued that higher perceived stability (PS) of the failure (likelihood of the failure reoccurring) would negatively impact customer loyalty (CL). The null hypothesis states that customer perception of the breach conditions as stable with not impact customer loyalty to the organisation. The alternative hypothesis states that customer perception of the breach conditions as stable will negatively an impact on customer loyalty (CL).

$H2_0$: $CL_{PS} - CL = 0$
$H2_1$: $CL_{PS} - CL > 0$

3.3. Controllability of Cause

Referring to the literature review above, it is argued that customers that perceive an organisation as having high control (C) over circumstances related to the data breach will dimmish their customer loyalty (CL). The null hypothesis states that customer perception of the breached organisations control over the data breach will have no impact on their customer loyalty to the organisation. The alternative hypothesis states that customer perception of the breached organisations control (C) over the data breach will negatively impact customer loyalty (CL).

$H3_0$: $CL_C - CL= 0$
$H3_1$: $CL_C - CL > 0$

3.4. Data Breach Severity

Based on the literature reviewed, the null hypothesis states Data breach severity (DBS) does not influence the relationship between perceived locus of causality (LC) and customer loyalty (CL). The alternative hypothesis states that Data breach severity (DBS) negatively influences the relationship between perceived locus of causality (LC) and customer loyalty (CL).

$H4_0$: Data breach severity (DBS) does not influence the relationship between perceived locus of causality (LC) and customer loyalty (CL).

$H4_1$: Data breach severity (DBS) negatively influences the relationship between perceived locus of causality (LC) and customer loyalty (CL).

Chapter 4: Research Methodology

4.1. Introduction

In this chapter, we discuss the research design and methodology used in the study. The chapter will touch on the aspects related to the research philosophy, the chosen methodology, the chosen population, the data gathering process and how reliability and validity were maintained in the study.

4.2. Choice of Methodology

Saunders and Lewis (2018) define a research philosophy as “the overall term that relates to the development of knowledge and the nature of that knowledge in relation to research” (p. 107). While there are five main philosophies, this study focused on understanding the impact of data breach severity on customer loyalty, the requirement was, therefore, to determine the causal effect of data breaches, by testing theory using structured quantitative methods which could be replicated and generalised. This was therefore in line with the Positivism research philosophy.

The research approach to theory development was deductive in nature and placed reliance on testing an established theory (Attribution Theory) using theoretical propositions and hypotheses followed by data collection, analyses and interpretation.

The methodology chosen was a mono-method quantitative study, where a single method was used to collect data. Since the research focused on a positivist paradigm, this focused the research towards quantitative methods (Azorín & Cameron, 2010). Azorin and Cameron (2010) state that mixed methods require more time, resources and effort than mono-methods, and due to the limited time in which the study was conducted (less than one year), a quantitative mono-method study was deemed to be more appropriate for the study.

This study adopted a descripto-explanatory design as it aimed to describe and analyse the variables under study and present their characteristics while explaining their relationship without manipulation as detailed by Saunders and Lewis (2018, p. 106).

The research strategy adopted was a between-subjects' experimental vignette design, where subjects were presented with carefully built scenarios to evaluate dependent variables including intentions, attitudes and behaviours (Aguinis & Bradley, 2014). This also allowed the researcher the ability to change and to control the independent variable which improved the reliability of the study (Aguinis & Bradley, 2014). Experimental vignettes are especially useful in studying nature and direction of causal relationships where the author needs to control the independent variable (Simmons, Carr, Hsu, & Shu, 2016)(Saunders & Lewis, 2012). Experimental vignette methodology (EVM) also allowed the author to understand behaviour intentions using scenarios that relate to sensitive themes (Aguinis & Bradley, 2014). This made experimental design appropriate for this specific study as it enabled the author to test the effect of the independent variables, namely data breach severity and locus of causality, on the dependent variable, behavioural intention (customer loyalty), for different groups of randomly selected customers in the population.

A 2X3 factorial design was used, where six varying scenarios regarding the severity of the data breach (high, medium, low) and underlying causes (external or internal) were proposed while all other variables were kept constant. A tabular representation of the research design is presented in table 1 below. Similar studies have used experiments to investigate data privacy impacts on customers (Martin et al., 2017).

Table 1: Tabular representation of research design

	Independent Variable 1: Locus of Causality	**Independent Variable 2: Severity**
Cell 1	Internal	Low
Cell 2	Internal	Medium
Cell 3	Internal	High
Cell 4	External	Low
Cell 5	External	Medium
Cell 6	External	High

The study took place at a single point in time, given the time constraints, thus making it cross-sectional using a mono-method approach. In addition, due to the study being a between-subjects design, this required that each participant be presented with only one randomly assigned vignette (Aguinis & Bradley, 2014). This was particularly appropriate as each subject was presented with one vignette, detailing a single scenario variation with regards to the severity of a data breach and a locus of cause at a single point in time, making a cross-sectional time horizon more appropriate for the study. The experiment was not be repeated in the study and no additional treatments were applied.

The data for the study was collected through an online self-completed questionnaire. Participants were presented with randomly assigned scenarios in the form of vignettes, in which they were requested to respond by answering a series of questions through a self-completed online survey. The self-completed survey had been identified as an effective and reliable method of data collection (Schoenberg & Ravdal, 2000).

4.3. Population

A population is defined as a “complete set of group members” (Saunders & Lewis, 2018, pp. 138-3). The population of the study was defined to be high net worth banking clients in South Africa, where high net worth clients were defined as individuals above the age of 18, earning an annual income of at least R500 000. While this may initially present as relatively low when compared to the global definition of one million dollars, this value was in line with the three highest income tax brackets as defined by the South African Revenue Service (SARS) and would serve as an approximation for high net worth based on the South African context (SARS, 2019). This value was also closely aligned with the minimum income required to qualify for a South African private banking account (Businesstech, 2019), and is also positioned to capture entry level clients into the South African Private Banking segment. Individuals were also expected to hold a South African bank account to form a part of the population.

The questionnaire presented the participant with a set of screening questions to ensure the participant fitted the qualifying criteria of the study, which was: that their

age was above 18, they were in possession of an active South African bank account and earned at least R500 000. Participants not meeting the criteria were initially thanked and not able to proceed with the questionnaire. However, during the pilot study to be discussed in section 4.7, some feedback was received from participants that the exclusion on income made the survey excessively short and caused confusion with some respondents. The survey was then amended not to filter for income, focussing on collecting all participant data, which could then be filtered during the analysis phase of the study.

4.4. Unit of analysis

The unit of analysis is viewed as the individual from which a researcher collects data from (Kumar, 2018). For this study, the unit of analysis was the high net worth individuals described in section 4.3 above i.e. individuals above the age of 18, who hold South African bank accounts and earn at least R500 000.

4.5. Sampling method and size

The sampling method that was used for the study was non-probability purposive sampling. This was achieved by “selecting units without replacement from the particular section of the population believed to yield samples that will give the best estimate of the population parameter of interest” (Guarte & Barrios, 2006, pp. 278-2). This sampling method was based on the researcher’s view of which participants are best placed to meet the objectives of the study and therefore, reflected the characteristics of the desired population (Etikan & Bala, 2017). The survey would be presented to individuals who were likely to satisfy the sampling frame (High net worth clients) like those currently studying in business schools and professionals. As this was an experiment, participants were presented with a single randomly assigned vignette. Once the survey was distributed to the initial population, non-probability snowball sampling was applied (Saunders and Lewis, 2018). This meant initial participants aided in identifying and sharing the questionnaire with other participants within their respective networks to achieve the required sample size. However, this method of sampling risked the introduction of a homogenous bias for the study, where the sample may not have been representative of the population (Fuller et al., 2016). This would be further discussed under the limitations section of the Chapter.

In determining an appropriate sample size for a subset of the population defined in Section 4.3, studies with similar methodologies were considered. It was noted that published academic articles using the experimental vignette methodology are limited (Aguinis & Bradley, 2014). However, Martin, Borah and Palmatie (2017) in their study titled *Data Privacy: Effects on Customer and Firm Performance* used 200 respondents for each of their three experiments using 50 participants for each vignette. In another recent pilot study investigating the *impact of data breach severity on post-breach online shopping intention*, Aivazpour, Valecha and Chakraborty (2019) utilised 56 participants for their experimental design studies. However, this pilot was only performed in preparation for a full-scale study and thus the sample size was determined based on convenience. Thus, consideration of similar studies that shared similarities in methodology (between-subjects experimental methodology) and key areas of study (i.e. customer behaviour), like the study by Martin, Borah and Palmatjie (2017), the sample size for the study was initially proposed to be 300 participants. This equated to 50 participants for each group, who would be presented with a single vignette describing a scenario of a data breach of varying severity and locus of cause.

In addition, VanVoorhi and Morgan (2007), suggest that large sample sizes better reflect the key characteristics of a population and increase the power of estimation. They recommend a sample size of approximately 50 participants per scenario when measuring relationships (correlations and regressions) to improve the power of estimation. However, they state that a minimum sample size of 30 per cell is appropriate for measuring groups differences. So, while the study sought to collect 50 responses per cell, the minimum number of respondents per cell was aligned to 30 individuals. This would be fulfilled through a self-administered online-based questionnaire. Table 2 below, provides a summary of the sample size determined for the study.

Table 2: Sample size

	Combination of independent variables	Sample size
Cell 1	LS + IL	50 (minimum 30)
Cell 2	MS + IL	50 (minimum 30)
Cell 3	HS + IL	50 (minimum 30)
Cell 4	LS + EL	50 (minimum 30)
Cell 5	MS + EL	50 (minimum 30)
Cell 6	HS + EL	50 (minimum 30)

4.6. Measurement instrument

A 2 (locus of causality: Internal, External) x 3 (severity: low, moderate and high) between-subjects experimental design was used to test the hypothesis. A stimulus (vignette) was presented to participants as per table 3 below, followed by an online self-administered questionnaire will be used to collect data for the study.

Participants were requested to answer the same questions after being presented with one of six randomly allocated data breach scenarios reflecting varying breach severities. The questionnaire included a brief introduction explaining the reason for the study, detailing participation as voluntary and confirming that data shared would be kept confidential. Data about the demographics of the participant would then be collected in line with the control variables detailed above, namely age, gender, Income, previous breach experiences and education level (Aivazpour et al., 2018). A screening pre-questionnaire was administered to determine that respondents met the requirements for the universe.

Once this was completed, the participant was randomly presented with one of six vignettes detailing a data breach compromise at their current bank, which will include details of the type and volume of customer data compromised. The measure for severity was borrowed from Aivazpour et al. (2018) where severity is defined using four elements: Number of breached records, Types of data, Source of the breach, and the Potential for the breached data to cause an individual, harm. These factors will be manipulated to reflect low exposure, moderate exposure and high exposure.

The vignettes are detailed below, with variables identify severity and locus of causality made bold along with a description of what they were representing in parenthesis. These were not highlighted to participants during the experiment to avoid the bias of responses during the completion of the survey. Table 3 below, presents the vignettes used in the study.

Table 3: Sample vignettes presented during questionnaire

Low Severity, Internal locus of causality Vignette
Your bank has recently announced that **1000 Records** *(severity - size of breach i.e. number of records)* have been stolen in a data breach. The information compromised included **email address and contact Information** *(severity - type of information).* In a recent media statement, the Bank advised that the data was compromised through **non-secure customer devices** *(Locus of causality)* and posed a **low *risk*** *(severity -potential for harm)* to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.
Moderate Severity, Internal locus of causality Vignette
Your bank has recently announced that **10 000 Records** *(severity - size of breach i.e. number of records)* have been stolen in a data breach. The information compromised included **bank account and credit card data** *(severity - type of information).* In a recent media statement, the Bank advised that the data was compromised through **non-secure customer devices** *(Locus of causality)* and posed **some risk** *(severity - potential for harm)* to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.
High Severity, Internal locus of causality Vignette
Your bank has recently announced that **over a million** Records (*severity - size of breach i.e. number of records)* have been stolen in a data breach. The information compromised included **bank account and credit card data** *(severity - type of information).* In a recent media statement, the Bank advised that the data was compromised **through non-secure customer devices** *(Locus of causality)* and posed **significant risk** *(severity - potential for harm)* to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.
Low Severity, External locus of causality Vignette

Your bank has recently announced that **1000 Records** (*severity - size of breach i.e. number of records)* have been stolen in a data breach. The information compromised included **email address and contact Information** *(severity - type of information).* In a recent media statement, the Bank advised that the data was compromised through **a malicious employee** *(Locus of causality)* and posed **low risk** *(severity - potential for harm)* to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.
Moderate Severity, External locus of causality Vignette
Your bank has recently announced that **10 000 Records** (*severity - size of breach i.e. number of records)* have been stolen in a data breach. The information compromised included **bank account and credit card data** *(severity - type of information).* In a recent media statement, the Bank advised that the data was compromised through a **malicious employee** *(Locus of causality)* and posed **some risk** *(severity - potential for harm)* to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.
High Severity, External locus of causality Vignette
Your bank has recently announced that **over a million** Records (*severity - size of breach i.e. number of records)* have been stolen in a data breach. The information compromised included **bank account and credit card data** *(severity - type of information).* In a recent media statement, the Bank advised that the data was compromised through a **malicious employee** *(Locus of causality)* and posed **significant risk** *(severity - potential for harm)* to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

For the questions in the questionnaire, the study used a seven-point Likert-scale, like other studies, where 1 represented a response of “highly unlikely” and 7 represented a response of “highly likely”. In some questions, 1 represented “strongly disagree” and 7 represented “strongly agree” (Martin et al., 2017). These were chosen as Seven-point Likert scales are affirmed to generate lower measurement error than the five- and three-point Likert scales (Barge, 2014). Also, they are considered especially effective for measuring attitudes as was the case in the study (Barge, 2014). Specifically, questions related to the locus of causality and controllability of cause were measured using a 7-point Likert-scale adapted from

Zhou and Ki (2018). Measures for questions related to Stability of cause were adapted from Huang (2010).

It was considered that reflecting all six hypotheses using a single vignette would result in an overly complex experiment and hence the study would measure some of the constructs (stability of cause and controllability of cause) through specific questions in the questionnaire and not explicitly reflected in the vignettes. In addition, questions related to the perceived control of respondents over their personal information was included in the questionnaire. these were not core to the overall study but would provide insight into customer perceptions which would enrich the data around data privacy for future studies. See appendix 1, questionnaire and consent form. An example of the questionnaire used in the Study is available in Appendix 1, which includes the consent form, breach scenario and questions measuring the various constructs.

4.7. Data gathering process

Supported by the measuring instrument above, the data gathering process followed included two phases – the pilot study and survey questionnaire. These will be discussed in detail below.

4.7.1. Pilot Study

A pilot study was constructed in line with similar studies (Aivazpour et al., 2018) where a small group of fewer than 10 participants who aligned with the profile of required participants, was presented with the survey to test for the effectiveness of the data collected, the clarity of the vignettes, validity and reliability of the instruments and any potential flaws in the experiment, before sending the questionnaire to a broader sample.

The pilot study highlighted minor changes related to the questionnaire, including additional clarity for the scenario framing, similarity of questions in some sections and minor wording changes that needed to be incorporated. These were subsequently addressed following the feedback received.

Once the pilot study had been completed, the self-administered online questionnaire was distributed to potential participants through a link that could be accessed through a smartphone, tablet or laptop. After acknowledging the consent form discussed in section 4.6, the questionnaire was completed using Google Forms. Participants were requested to complete a sequence of questions in line with constructs of customer loyalty as the dependant variable. There were six sections to the questionnaire, titled: Consent, Background, Breach Scenario, The cause of the breach, Control over your personal information and your response to the data breach. Each section had questions related to the title. The questionnaire remained open for two months to obtain the minimum required number of respondents for each vignette (30). However, this time frame was extended due to under-subscription of qualifying responses. Once the required sample size was achieved, the survey was closed, and results analysed.

4.7.2. Addressing a shortage in survey responses

After an initial evaluation of the number of responses collected and the researchers attempts to increase the number of respondents by further distributing the survey through social media channels like WhatsApp, Facebook and Linked In, the researcher then boosted the sample by distributing the survey to identified members of his organisation. Cells that had already satisfied the required minimum number of 30 respondents were removed from selection. This was done to satisfy the minimum number of responses required for each vignette in the study. This increased the total number of qualifying responses. However, this remained lower than the number initially envisaged at the onset of the study (50 respondents). Table 4 below summarises the total respondents obtained.

Table 4: Survey Reponses

	Cell 1	Cell 2	Cell 3	Cell 4	Cell 5	Cell 6	Disqualified responses
Initial Survey	20	18	21	62	2	8	101
Boosted Sample	14	16	18	0	30	45	63
Total	34	34	39	62	32	53	164

Due to time constraints, it was then considered that the study would continue with the data collected as the minimum number of respondents as set out in the study had been met data. However, this slightly reduced sample size introduced the risk of the sampled respondents not sufficiently reflecting the population under study and in turn limiting the generalizability of the results (Aguinis & Bradley, 2014). However, VanVoorhis and Morgan (2007), state that as a general rule, a reasonable sample size for measuring group differences (ANOVA, t-test), is 30 respondents per cell and will lead to statistical power pf about 80% when conducting tests. They further state that the absolute minimum respondent should not be less than seven per cell. Notably, they further stress that power of the tests increases as the total number of respondents per cell increase (Vanvoorhis & Morgan, 2007). Thus, the sample was deemed suitable for the study.

Additional tests were applied during the analysis done in chapter five to understand the impacts, if any, of this reduced sample.

4.7.3. Coding

For the purposes of analysis in the study, the below coding was applied to facilitate further analysis of the data gathered in the study:

- Age group: 1 = 18-24, 2 = 25-34, 3 = 35-44, 4 = 45-54, 5 = 55-64, 6 = 65+
- Gender: 1 = Male, 2 = Female, 3 = Prefer not to say
- Highest level of education: 1 = Below Grade 12, 2 = Grade 12 - Matric, 3 = College diploma, 4 = Bachelor's degree, 5 = Honours degree or equivalent, 6 = Master's degree, 7 = Doctoral degree
- Annual gross salary: 1 = below R100 000, 2 = R100 000 - R299 000, 3 = R300 000 - R499 000, 4 = R500 000 - R699 0000, 5 = R700 000 - R899 000, 6 = R900 000 - R1.1 Million, 7 = more than R1.1 Million
- Banking Institution: 1 = Absa Group Limited, 2 = African Bank, 3 = Capitec Bank, 4 = Discovery Bank, 5 = First National Bank, 6 = Investec Bank, 7 = Rand Merchant Bank, 8 = Nedbank, 9 = Post Bank, 10 = Standard Bank, 11 = Tyme Bank, 0 = Other
- Victim of a data breach: 1 = Yes, 0 = No

- 7-point Likert scale questions: 1 = Highly unlikely, 2 = Unlikely, 3 = Somewhat unlikely, 4 = Neutral, 5 = Somewhat likely, 6 = Likely, 7 = Highly likely
- 7-point Likert scale questions: 1 = Strongly disagree, 2 = Disagree, 3 = Somewhat disagree, 4 = Neither agree nor disagree, 5 = Somewhat agree, 6 = Agree, 7 = Strongly agree

4.8. Analysis approach

The responses to the questionnaire were downloaded onto Microsoft Excel and uploaded into IBM SPSS for further analysis (Saunders and Lewis, 2018). It was determined that some respondents had not completed the questionnaire and thus only participants that submitted responses to all the mandatory questions had been included in the analysis.

The descriptive statistics were then computed based on the demographic variables collected to provide details around the characteristics of the sample, along with tests on normality (mean, variance, standard deviation) and the five-number summary (Vanvoorhis & Morgan, 2007). The responses to questions under each construct were analysed for reliability using Cronbach's Alpha, composite reliability and AVE scores based on a similar studies (Aivazpour et al., 2018). This extended to manipulation checks which were used to test the effectiveness of the independent variable (Aivazpour et al., 2018). The results of the calculations are presented in Chapter five.

Aguinis and Bradley(2014) state that as part of the analysis process for between-subjects' experiments, data techniques like ANOVA and regression are recommended, and were considered for this study. An independent t-test along with regression analysis was used to analyse the significance of the relationships. ANOVA and t-test are designed to detect differences (Vanvoorhis & Morgan, 2007).

In the study, hypothesis one and four were tested using the two-way ANOVA, in line with the General Linear Model procedure in SPSS. These are statistical tests that measure if there is a significant difference in means between two or more independent groups (Hair, Black, Babin, & Anderson, 2007). To test hypothesis two and three the study used Structural Equation Modelling which is useful for analysing

interrelated measures or relationships within a system and determining covariance between the variables (Hair et al., 2007). This was performed using IBM SPSS Amos 26.

4.9. Quality controls

The quality controls to assure quality data was collected were achieved by introducing a pilot study, discussed in section 4.7.1 above, where the vignettes and questionnaire were distributed to a small pilot group to test for issues prior to distributing the questionaire widely.

4.9.1. Internal and external validity

Validity can be defined as “the extent to which data collection methods measure what they are intended to measure” (Saunders & Lewis, 2018, pp. 134-3). Any issues determined during this phase will be promptly addressed. For an experiment to be considered valid, it must with a high degree of certainty show that the causal relationship established is only due to the manipulated variables of the study and not influenced by other variables outside of the study (internal validity) (McDermott, 2011). In addition, it should generate results that can be generalised to other contexts and environments (external validity) (McDermott, 2011).

For the study, internal validity was increased by increasing the amount of information and realism presented in the vignette, making it more realistic (Aguinis & Bradley, 2014). This was achieved by testing the proposed vignettes with banking industry experts during the pilot study described in the data gathering process. In addition, the experiment was also addressed, by limiting the factors changed in each vignette to ensure changes in behaviour were due to a single phenomenon. Lastly, to avoid attrition, a minimum number of respondents will be required for each vignette presented (McDermott, 2011). External validity was achieved through randomly assigning each participant to a vignette. The manner in which samples were chosen was one of the methods which had previously been used to improve the external validity of a vignette study (Simmons et al., 2016).

4.9.2. Reliability

Reliability is a concept defined by Saunders and Lewis (2018, p. 135) as the extent to which data collections methods and analysis procedures will produce consistent results. For the study, reliability was measured using Cronbach's alpha (Cronbach's α), which measures internal consistency and how the related items are, as a group (Bonett & Wright, 2015). It ranges between 0 and 1, with values closer to 1 representing a high level of reliability. It has been extensively used as a measure for the reliability of scales when the questionnaire has multiple test items (Bonett & Wright, 2015). According to Bonett and Wright (2015), the acceptable reliability value depends on the application. However, similar studies have considered the minimal accepted level at 0.7 for scale robustness (Chen, 2015; Huang, 2008). The study adopted 0.7 as the minimum reliability value.

In addition, the scale was optimised to ensure high reliability by removing scales that decrease the reliability value. This is computed in chapter five.

Purposive sampling, by its nature, introduces bias, as it samples based on the researcher's knowledge, and is a type of non-probability sampling (Etikan & Bala, 2017) which may yield different results depending on the sample chosen. However, Guarte and Barrios (2017) state that purposive sampling can yield reliable results even in vastly different populations. The study further addressed external validity by ensuring a sufficiently large sample size (at least 30 respondents per vignette) to be more reflective of the population in scope.

4.10. Limitations

While the scenarios that were presented in the study enhance the knowledge on the impact of data breach severity on customer loyalty through experiment, the experimental vignette method is regularly criticized for its limited ability to be used in generalisation, as subjects are presented with hypothetical scenarios (Simmons et al., 2016). Aguinis and Bradley (2014) suggest that this can be overcome by first ensuring that the vignette is designed to present subjects with enough information for context, and secondly improving the immersion by making it more realistic which was considered in this study. Furthermore, great care was taken to frame scenarios

as realistic using pervious framings of the independent variables (Aivazpour et al., 2018; Stiennon, 2013) and the pilot study, but potential errors in respondents misinterpreting the detail was noted as a possible limitation of the study.

It should also be noted that the dependant variable, namely customer loyalty, comprises of constructs and behaviours that may occur over time, and while a point-in-time study is sufficient for studying this variable based on previous studies (Martin et al., 2017), further changes in customer loyalty intention may not be fully captured in the study. This along with other limitations will be elaborated on further in Chapter seven.

Chapter 5: Results

5.1. Introduction

The study aimed to understand the impact of data breaches, of varying severity, on the loyalty of retail banking clients. This would be achieved by establishing a causal relationship between data breaches and their customer loyalty intention.

This chapter provides the complete analysis results and insights of the experiment conducted through the survey approach discussed under the methodology section in Chapter four. This chapter begins by including a brief description of the characteristics of the sample considered. The analysis results of each hypothesis identified in chapter three will then be presented. Additional tests performed will also be discussed. The section is then concluded with a summary of the key results obtained.

5.2. Sample size and data preparation

In line with the 2 X 3 factorial design discussed in the methodology section, six groups of subjects completed the survey with a randomly assigned breach scenario. Each group satisfied the minimum number of respondents required (30). The samples were therefore deemed credible to perform tests that have sufficient statistical power.

A total of 418 responses were collected (254 after filtering inadmissible responses). These responses were gathered in two tranches. The initial distribution was supplemented with the boosted sample which was mainly made up of people within the author's employment network.

Both data sample outputs were downloaded from Google Forms into Microsoft excel with an indicator of 1 or 2 included (to identify which sample the data was collected from) prior to being merged for analysis. Of the data collected, 144 responses were disqualified due to not satisfying the minimum income criterion of R500 000. A further 20 were disqualified for completing less than 50% of the survey. The disqualified

responses were then removed from the data set. Once the data set had been purged of non-qualifying responses, each remaining response was then coded to reflect the combination of independent variables it had been exposed to during the survey, thus creating six different groupings in line with the design presented in Chapter four. This was a combination of severity (low, medium, high) and Locus of causality (external or internal) i.e. LS +EC. Table 5 summarises the total data collected and used for analysis in the chapter.

Table 5: Sample size collected

	Combination of independent variables	Sample size
Cell 1	LS + IL	34
Cell 2	MS + IL	34
Cell 3	HS + IL	39
Cell 4	LS + EL	62
Cell 5	MS + EL	32
Cell 6	HS + EL	53

Once the data had been coded, it was then combined to perform the analysis that is discussed in the remainder of the chapter.

5.2.1. Testing impact of Boosted samples

To determine if the two samples resulted in a statistically significant difference, an independent T-test was used. This was to determine if both samples were drawn from the same population. That is, testing whether the mean of the initial sample is equal to the mean of the boosted sample. The null hypothesis is stated below:

H_0: $\mu_{Sample\ 1} - \mu_{boosted\ sample} = 0$

The results of the T-tested are summarised in Table 6. These were determined at a significance level of 95%. The results show that there is no statistically significant difference between the two-sample means (P= 0.249, t=1.15). This means the study failed to reject the null hypothesis. The study therefore concludes that the first sample

and the boosted sample in the study can be said to have been drawn from the same population, and combining the two samples is plausible for analysis.

Table 6: Independent Samples T-test

		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Customer Loyalty Intention	Equal variances assumed	.001	.979	-1.154	252	.249	-.25030	.21684	-.67734	.17674
	Equal variances not assumed			-1.155	251.138	.249	-.25030	.21680	-.67729	.17668

5.3. Description of demographics

This section provides an overview of the demographical information of the respondents. Table 7 provides an overview of demographic information. It is worth noting that the demographic information of all survey participants was complete.

Within the sample, the following is evident:

- 41% of respondents identified best with the Female gender description compared to 59% who identified with the Male. A single participant preferred not to state their Gender.
- The sample is skewed towards the ages of 25 and 54, with 94% of participants falling within this age range.
- For income, 26% of the qualifying respondents answered that they exceeded the upper bound of income by earning more than R1.1 million. A further 15% responded that they earn between R900 – R1.1 Million.
- In terms of the banking institutions, 58% of the sample were primary banking clients of First National Bank. The other major banking institutions included Standard Bank, Absa Group Limited, Investec Bank and Capitec Bank with 12%, 9%, 7% and 6% respectively. It was determined that the increased number of FNB respondents was attributed to the booster sample. This will be elaborated on further in the chapter.

- Details of the previous breach experience of respondents showed that 38% of respondents had previously been victims of a data breach(s). Of those who reported having experienced a breach, 60% confirmed that Personal identifiable information (name, email, contact details, identity numbers, address) had been compromised.

Table 7: Demographic details of respondents

		Total Count	%
Gender	Female	104	41%
	Male	149	59%
	Prefer not to say	1	0%
Age	18-24	3	1%
	25-34	109	43%
	35-44	88	35%
	45-54	43	17%
	55-64	11	4%
Education	Below Grade 12	1	0%
	Grade 12 - Matric	11	4%
	College diploma	24	9%
	Bachelor's degree	74	29%
	Honours degree or equivalent	86	34%
	Master's degree	52	20%
	Doctoral degree	6	2%
Income	R500 000 - R699 0000	82	32%
	R700 000 - R899 000	67	26%
	R900 000 - R1.1 Million	38	15%
	more than R1.1 Million	67	26%
Bank	Absa Group Limited	23	9%
	Capitec Bank	14	6%
	Discovery Bank	1	0%
	First National Bank	148	58%
	Investec Bank	18	7%
	Nedbank	9	4%
	Other	2	1%
	Rand Merchant Bank	8	3%
	Standard Bank	31	12%

Table 8: Respondent demographics per category

		Group 1		Group 2		Group 3		Group 4		Group 5		Group 6	
	Option	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%
Gender	Female	13	38%	14	41%	17	44%	33	53%	12	38%	15	33%
	Male	21	62%	20	59%	22	56%	28	45%	20	63%	30	67%
	Prefer not to say							1	2%				
Age	18-24	1	3%		0%		0%	1	2%	1	3%		0%
	25-34	8	24%	19	56%	15	38%	36	58%	11	34%	20	38%
	35-44	13	38%	7	21%	16	41%	16	26%	15	47%	21	40%
	45-54	9	26%	6	18%	7	18%	7	11%	3	9%	11	21%
	55-64	3	9%	2	6%	1	3%	2	3%	2	6%	1	2%
Education	Below Grade 12	1	3%		0%		0%		0%		0%		0%
	Grade 12 - Matric	3	9%		0%	2	5%	3	5%	1	3%	2	4%
	College diploma	3	9%	1	3%	8	21%	5	8%	2	6%	5	9%
	Bachelor's degree	8	24%	10	29%	7	18%	21	34%	11	34%	17	32%
	Honours degree or equivalent	7	21%	15	44%	16	41%	23	37%	8	25%	17	32%
	Master's degree	10	29%	8	24%	6	15%	9	15%	9	28%	10	19%
	Doctoral degree	2	6%		0%		0%	1	2%	1	3%	2	4%
Income	R500 000 - R699 0000	16	47%	8	24%	13	33%	20	32%	9	28%	16	30%
	R700 000 - R899 000	9	26%	9	26%	9	23%	18	29%	11	34%	11	21%
	R900 000 - R1.1 Million	5	15%	6	18%	2	5%	11	18%	3	9%	11	21%
	more than R1.1 Million	4	12%	11	32%	15	38%	13	21%	9	28%	15	28%
Bank	Absa Group Limited	4	12%	3	9%	4	10%	5	8%	2	6%	5	9%
	Capitec Bank	4	12%	3	9%	1	3%		0%	4	13%	2	4%
	Discovery Bank		0%	1	3%		0%		0%		0%		0%
	First National Bank	18	53%	13	38%	25	64%	43	69%	20	63%	29	55%
	Investec Bank		0%	4	12%	2	5%	4	6%	3	9%	5	9%
	Nedbank	1	3%	1	3%		0%	4	6%	2	6%	1	2%
	Other	1	3%		0%	1	3%		0%		0%		0%
	Rand Merchant Bank	1	3%	2	6%	3	8%		0%		0%	2	4%
	Standard Bank	5	15%	7	21%	3	8%	6	10%	1	3%	9	17%

Table 8 provides an overview of the demographics of respondents based on the randomised group they formed a part of during the study. In each group, male respondents were in the majority excluding group 4 where female respondents exceeded male, 53% and 45% respectively. Most respondents were within the 25-34 and 35-44 age groups. Like the overall sample, respondents had a minimum of a bachelor's degree across all groups. Income was also similarly distributed across the age groups. First National Bank was identified as lead bank, with at least 50% of respondents deeming them their Primary banking institution. This will be analysed further to rule out bias.

5.4. Defining the measures for independent and dependant variables

For the purposes of the study, multi-scaled ratings were used to measure two of the four independent variables, namely the stability of cause and the controllability of the breach, in line with similar studies which had used similar constructs (Huang, 2008; Zhou & Ki, 2018). Moreover, an additional multi-scaled measure for the locus of causality was included over and above the one presented in the experiment. This was done to ensure that the interpretation of the locus of causality was well understood by respondents. This would also be used to test the robustness of the scenarios presented to test the locus of causality i.e. for scenarios presented to show

an internal locus of causality, was the respondents understanding of this congruent with their responses to subsequent questions in the survey designed to determine an internal locus – executed through multiple rating scales.

The dependent variable measured customer loyalty intention following the breach event is also determined using multiple rating scales, and for the purposes of further analysis and interpretation of results, these are defined below.

5.4.1. Dependent Variable: Customer loyalty intention

The dependent variable, namely customer loyalty, was measured using nine questions related to a combination of repeat purchase intention, word of mouth and switching behaviour intention. These were the primary constructs related to customer loyalty as identified by the literature. The scales were then combined, summed and averaged, to establish a single measure for loyalty intention utilising summed rating scales.

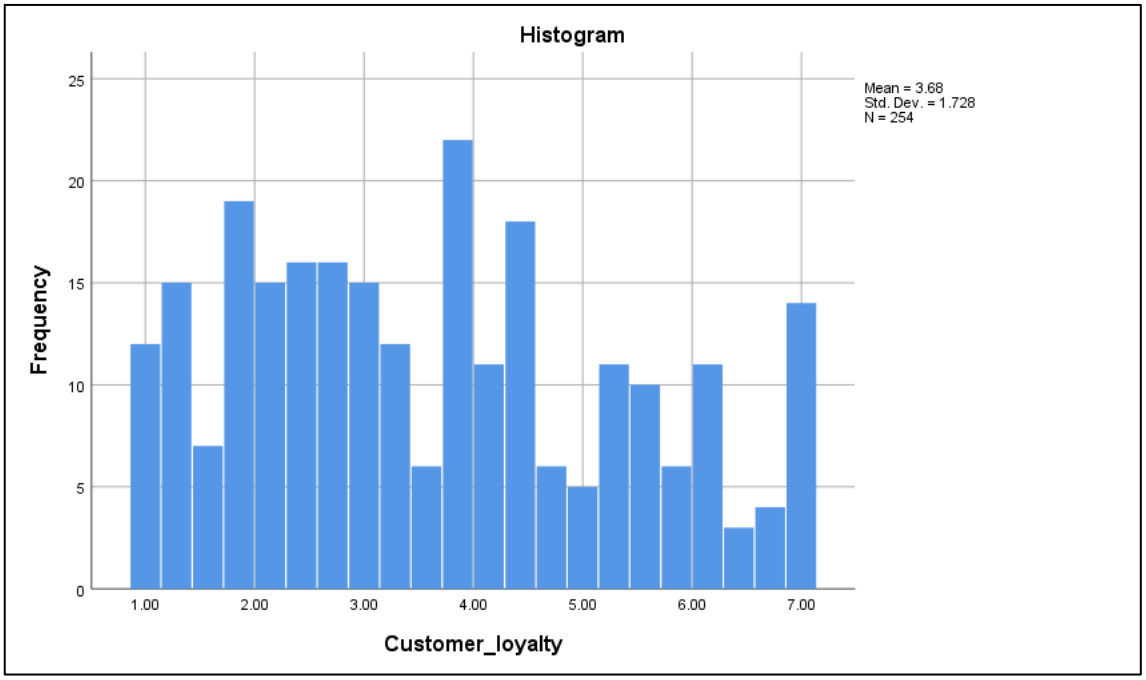
To satisfy the conditions required to perform ANOVA tests, a test for normality was conducted to determine if customer loyalty intention was normally distributed using both the Kolmogorov Smirnov test and the Shapiro-Wilk at a p-value = 0.05. A p-value above 0.05 would not be statistically significant and thus the study would fail to reject the null hypothesis that customer loyalty intention is normally distributed. The results of both tests are reflected in table 9 below and show that customer loyalty intention is not normally distributed (P=0.001 and P= 0.000). Furthermore, the data was positively skewed (skewness = 0.319).

Table 9: Tests of Normality for Customer loyalty intention

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Customer loyalty Intention	.078	254	.001	.956	254	.000

a. Lilliefors Significance Correction

Figure 2: Histogram of customer loyalty intention



The other condition required to run an ANOVA test relates to equality of variances within groups (Hair et al., 2007). Levene's test for equality of means was conducted when testing the reliability of the scales in section 1.4 and the assumption for equality of means was met (P-value = 0. 274) – equal variances are assumed. Table 11 summarises the outcomes of Levene's test.

The last condition required that all samples be drawn independently, which was satisfied through the data gathering process of the between-subjects' study. Thus, two of the three conditions for hypothesis testing using ANOVA were met. However, Hair, Black, Babin and Anderson (2007) states that in assessing the impact of the violation of the normality assumption, the sample size must be considered (p.70). They state that the effects of non-normality are significantly reduced for samples sizes greater than 200 (Hair et al., 2007). Further to this, they state that when sample sizes are large, researchers should be less concerned about non-normal distributions (Hair et al., 2007). Based on this, the study continued with the tests for ANOVA despite violating the normality condition i.e. one of the three requirements.

Next, the study then considers the scales for the independent variables.

5.4.2. Independent variable: Locus of causality

The independent variable of locus of causality was measured using wording that reflected an internal or external locus of causality. The breach scenario was reflected as external or internal based on the scenario randomly assigned. However, following the scenario presented, the first set of questions respondents were required to answer related to their understanding of the locus of causality. This was to test the robustness of the scenarios presented.

These subsequent questions (measurement scales) were combined and averaged to form a second measure for the perceived locus of causality and, for the analysis, was interpreted as follows:

- External Locus: mean score of 4.1 or higher
- Internal Locus: mean score lower than 4

5.4.3. Independent variable: Stability of Cause

The independent variable of stability of cause was measured using two questions previously used in other studies to measure the stability of cause(Huang, 2008). The rating scales were reverse-coded, summed and averaged to complete a measure of stability – summated rating scale. To interpret the results, the following applies:

- Unstable Stable cause: mean score of 4.5 or higher
- Neutral stability: Mean score of 4 – 4.4
- Sable cause: unstable cause: mean score lower than 4

5.4.4. Independent variable: Controllability of Breach

The independent variable of perceived controllability of breach was measured using four questions. The questions were reverse-coded and combined in line with summated rating scales to obtain the measure for perceived controllability of the breach. To interpret the results, the following applies:

- Controllable cause: mean score of 4.5 or higher
- Neutral controllability: Mean score of 4 – 4.4
- Uncontrollable cause: mean score lower than 4

5.5. Scale reliability

The independent variables of perceived locus of causality, stability of breach and controllability of data breach are all measured utilising a multi-item scale composed of several questions for each variable. Hair, Black, Babin and Anderson (2007) state that "summed-scales combine several variables that measure the same concept into a single variable to increase the reliability of the measurement" (p. 3). Moreover, the measure for the dependent variable of customer loyalty is also measured using a multi-item scale. The questions were derived from previous similar studies to ensure proven reliability. To assess the reliability of the scales in this study, Cronbach's alpha values were computed and provided in table 10 below:

Table 10: Cronbach's alpha for the reliability of scales

Measure	Cronbach's α	Number of items
Locus of Control	.912	4
Stability of Cause	.621	2
Controllability of Cause	.878	4
Customer Loyalty	.928	7

The alpha value for Locus of causality (α = 0.912), Controllability of cause (α = 0.878) and customer loyalty (α = 0.928) exceed the recommended reliability measure of 0.7 which was quoted in earlier sections. Specifically, for the reliability measure of customer loyalty, it was shown that reducing the sale by excluding 2 items would increase the reliability measure - with this exclusion, the measure reduced from 9 to 7. See appendix 3.

The reliability measure for the perceived stability of cause was α = 0.621 which is lower than the recommended reliability measure of previous studies. This is mainly due to the limited items within the measure. However, Hair, Black, Babin and Anderson (2007) states that an accepted limit of above 0.6 will still provide reliable

scores (p140). In addition, Bonnet and Wright (2015) state that while the general rule is α > 0.7 for a reliability score, type of application is more important when determining an acceptable level. Based on this, the study then accepted the reliability measure of 0.621 for the perceived stability of cause as sufficient to test hypothesis, but this would be noted in the conclusion as a potential focus for future studies where additional measures would be required to further capture the phenomenon under study.

Homogeneity of Variances

Lavene's test was used to test the assumption of homogeneity of variance. This tests whether the variances of two or more samples are approximately equal. Interpretation of the test was that a P-value of greater than 0.05 would imply that equal variances were to be assumed. The below table 11 shows the results of Levene's test for the study, where a p-value of 0.274, which means the assumption of equal variances has been satisfied.

Table 11: Levene's Test for Equality of Variances

Test of Homogeneity of Variance					
		Levene Statistic	**df1**	**df2**	**Sig.**
Customer loyalty	**Based on Mean**	1.277	5	248	.274
	Based on Median	.875	5	248	.499
	Based on Median and with adjusted df	.875	5	241.284	.499
	Based on trimmed mean	1.258	5	248	.283

5.6. Descriptive statistics

In this section, we compute the descriptive statistics for the total sample by considering the independent and dependents variables. The independent variables of perceived locus of causality, perceived stability of cause and perceived controllability are described first, followed by the dependent variable of customer loyalty. All variables were measured using a multi-item scale. To calculate the

descriptive statistics items within each rating scale were averaged to produce an index, which will be used in to compute descriptive statistics split by varying demographic data.

5.6.1. Perceived locus of Causality

A four item-rating scale was used to calculate the perceived stability of cause (second measure). The items were subsequently averaged to define an index for perceived stability of cause as described in section 1.5 above. Table 12 summaries the results of the total sample by considering the perceived locus of causality.

Table 12: Descriptive statistics for Perceived Locus of Causality

	N	Mean (M)	Std. Deviation	Median	Skewness
Total Sample	254	5.4035	1.45636	5.8333	-1.179
Age					
18-24	3	6.1111	0.09623	6.1667	-1.732
25-34	109	5.5092	1.39163	5.6667	-1.354
35-44	88	5.3333	1.42993	5.75	-1.079
45-54	43	5.2752	1.55706	6	-0.949
55-64	11	5.2273	2.08603	6.1667	-1.124
Gender					
Female	104	5.3413	1.46339	5.6667	-1.121
Male	149	5.4362	1.45408	5.8333	-1.233
Prefer not to say	1	7	.	7	.
Income					
R500 000 - R699 0000	82	5.2195	1.28377	5.5	-0.9
R700 000 - R899 000	67	5.398	1.47338	5.6667	-1.338
R900 000 - R1.1 Million	38	5.557	1.45104	6	-1.232
more than R1.1 Million	67	5.5473	1.63706	6	-1.402
Primary Bank					
Absa Group Limited	23	5.7464	1.12352	6	-1.483
Capitec Bank	14	5.4762	1.49194	5.8333	-1.007
Discovery Bank	1	4	.	4	.
First National Bank	148	5.1667	1.5151	5.5	-1.022
Investec Bank	18	5.6574	1.32777	5.5833	-1.483
Nedbank	9	6	1.27203	6.3333	-1.887
Other	2	6.1667	0.2357	6.1667	.
Rand Merchant Bank	8	5.2917	1.49801	6	-1.04

Standard Bank	31	5.9516	1.36368	6.1667	-2.202

Based on the interpretation scale provided in section 1.4.1 of chapter five for the perceived locus of causality, the results show that respondents despite age, gender or income tended to perceive the locus of causality of the breach as external in nature. There is minimal variation by the primary banking institution, except for respondents from Discovery Bank who showed a neutral perception of the cause of the breach when compared to the other banks. This could be as a result of the sample– a single participant was recorded from Discovery Bank. Furthermore, the table below highlights that this perception of an external locus of causality (the breached bank), was maintained despite the survey scenario suggesting that the cause may be internal in nature.

Figure 3: Histogram of the second measure for the Perceived locus of Causality

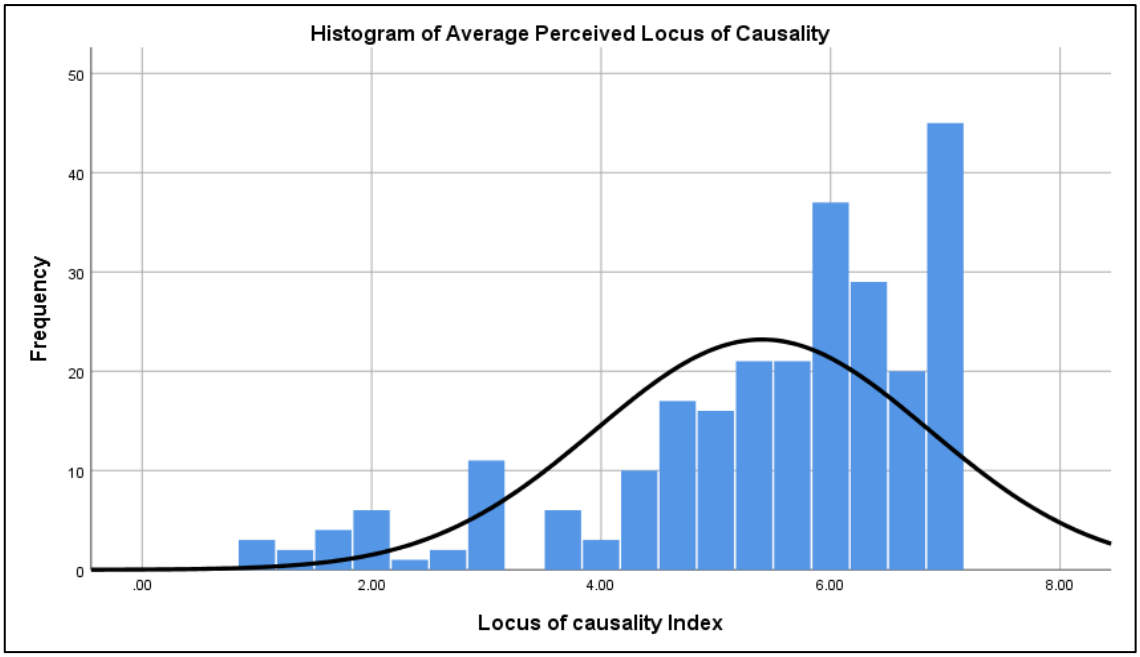


Figure 3 above, highlighted that respondents tended to view the causes of the breach as being caused by an external cause, despite a randomised combination of external and internal causes being presented in the scenario. This was further explored in Table 13 below.

Table 13: Descriptive statistics for Perceived Locus of Causality by Measures of locus of causality presented in the experiment

	N	Mean	Std. Deviation	Median	Skewness
External Locus	147	5.6474	1.33312	6.0000	-1.483
Internal Locus	107	5.0685	1.55523	5.3333	-.866
Total	254	5.4035	1.45636	5.8333	-1.179

Table 13 highlights that customers that we presented with an internal locus of cause scenario, it was still evaluated as being an external locus of cause. This could be a result of two reasons. 1) Respondents did not adequately understand the internal locus scenario presented. 2) Respondents had a bias to associate the results of negative news like the breach to an external locus as previously determined in the literature review (hedonic bias)(Weiner, 1985).

5.6.2. The Perceived Stability of Cause

The perceived stability of the cause of the breach (likelihood of occurring in the future) was measured using a summed-scale with two rating scales. These scales were summed and subsequently averaged to create an index for the perceived stability of the breach cause. The descriptive results of the sample related to the perceived stability of cause are presented below:

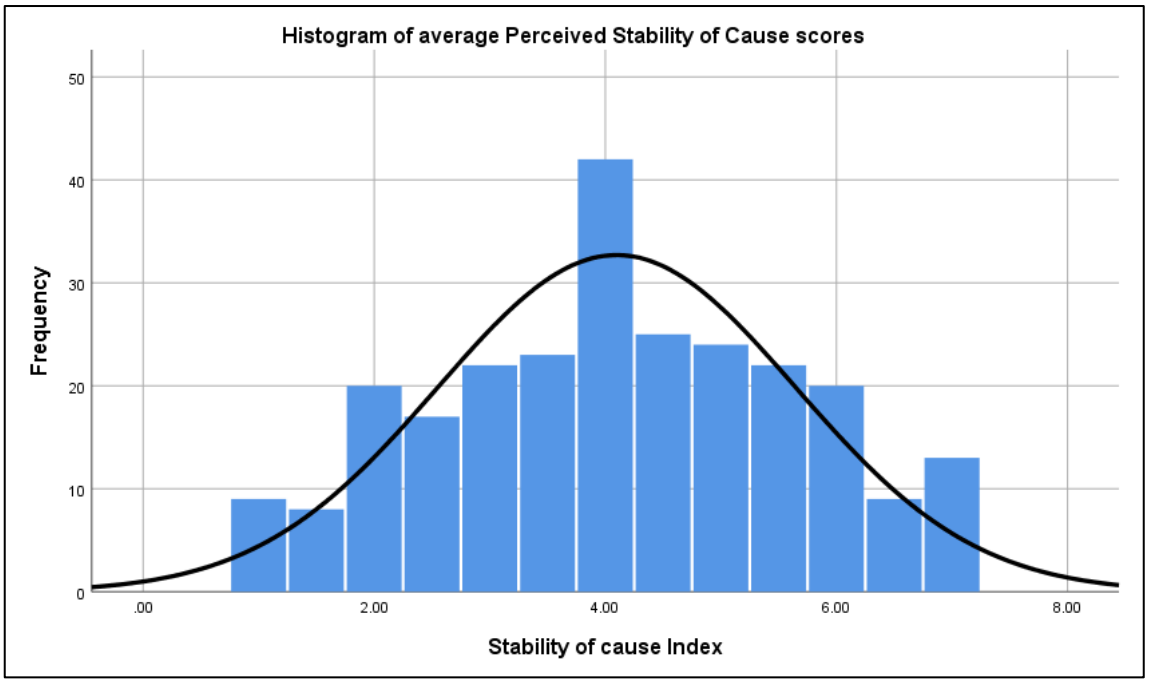
Table 14: Descriptive statistics for Perceived Stability of Cause

	N	Mean (M)	Std. Deviation	Median	Skewness
Total Sample	254	4.0984	1.5496	4.0000	-0.0390
Age					
18-24	3	4.1667	1.2583	4.0000	0.5860
25-34	109	4.4495	1.4735	4.5000	-0.2640
35-44	88	3.8409	1.5039	4.0000	0.1530
45-54	43	3.7558	1.6452	3.5000	0.1950
55-64	11	4.0000	1.8708	4.0000	0.0560
Gender					
Female	104	4.1154	1.5028	4.0000	0.0580
Male	149	4.1007	1.5822	4.0000	-0.1070
Prefer not to say	1	2.0000	.	2.0000	.

Income					
R500 000 - R699 0000	82	4.1220	1.5646	4.0000	-0.1430
R700 000 - R899 000	67	4.0672	1.7772	4.0000	-0.0430
R900 000 - R1.1 Million	38	4.2500	1.3036	4.0000	0.1790
more than R1.1 Million	67	4.0149	1.4380	4.0000	0.0990
Primary Bank					
Absa Group Limited	23	4.4783	1.6059	4.5000	-0.7050
Capitec Bank	14	5.0357	1.4867	5.0000	-1.3920
Discovery Bank	1	4.5000	.	4.5000	.
First National Bank	148	3.8480	1.5460	4.0000	0.2210
Investec Bank	18	4.5278	1.2773	4.7500	-0.1890
Nedbank	9	4.2778	1.2528	4.0000	0.0380
Other	2	5.5000	1.4142	5.5000	.
Rand Merchant Bank	8	3.8125	1.3346	3.5000	0.3560
Standard Bank	31	4.2581	1.6526	4.0000	-0.1810

The perceived stability of cause reflected a slightly negative skewed when computed, although reflecting a more negative distribution when computed in the histogram in figure 4 below. However, based on the interpretation scale provided previously, this meant respondents tended to be more neutral around the likelihood of the breach recurring in future. This perception was more neutral in ages 18- 34 and reduced with an increase in age bands, where respondents perceived the breach as unlikely to occur in future. Gender and Income tended towards a similar neutral view. The results further showed that respondents from different banking institutions varied in their perceived view of the breach recurring, with respondents from FNB and RMB reflecting slightly positively skewed perceptions of stability when compared to those of the other banking including ABSA, Capitec, Investec and Discovery who tended to be more neutral.

Figure 4: Histogram of the Perceived Stability of Cause mean scores



5.6.3. Perceived Controllability of Cause

There perceived controllability of the data breach case was measured using a 4-item rating scale. Like the other independent variables in the study, it was summed and averaged to generate an index for the perceived controllability of the data breach cause. This is computed in table 15 below:

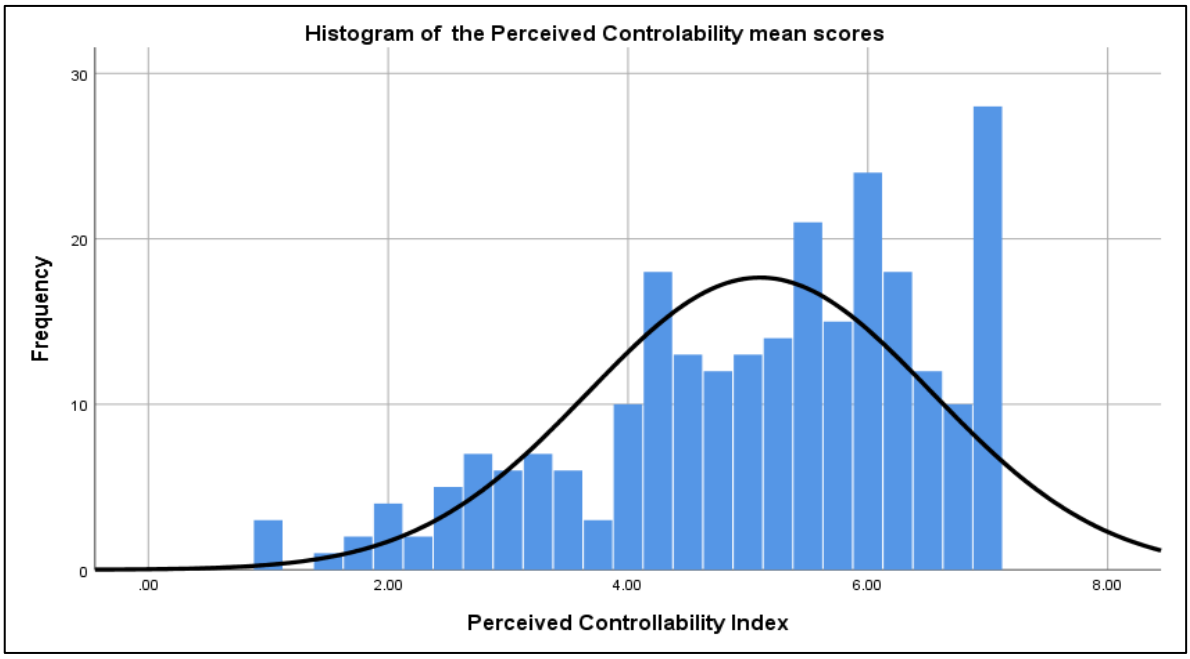
Table 15: Descriptive statistics for Perceived Controllability of Cause

	N	Mean (M)	Std. Deviation	Median	Skewness
Total Sample	254	5.1004	1.4346	5.5000	-0.6920
Age					
18-24	3	5.4167	1.0408	5.7500	-1.2930
25-34	109	5.1124	1.4083	5.2500	-0.8290
35-44	88	5.0341	1.3673	5.1250	-0.4720
45-54	43	5.2151	1.6606	5.5000	-0.7750
55-64	11	4.9773	1.5631	5.7500	-0.9580
Total	254	5.1004	1.4346	5.5000	-0.6920
Gender					
Female	104	4.9639	1.4977	5.2500	-0.6670
Male	149	5.2081	1.3817	5.5000	-0.7180
Prefer not to say	1	3.2500	.	3.2500	.
Total	254	5.1004	1.4346	5.5000	-0.6920
Income					

more than R1.1 Million	67	5.1082	1.4250	5.5000	-0.7630
R500 000 - R699 0000	82	4.9665	1.3877	5.2500	-0.4310
R700 000 - R899 000	67	5.1940	1.6054	5.7500	-1.0090
R900 000 - R1.1 Million	38	5.2105	1.2527	5.3750	-0.2920
Total	254	5.1004	1.4346	5.5000	-0.6920
Primary Bank					
Absa Group Limited	23	5.2174	1.4892	5.7500	-0.8590
Capitec Bank	14	5.4464	1.8402	6.0000	-1.6260
Discovery Bank	1	3.5000	.	3.5000	.
First National Bank	148	4.9696	1.4157	5.0000	-0.5100
Investec Bank	18	5.2778	1.2423	5.2500	-0.4040
Nedbank	9	4.8889	1.3176	5.2500	-1.2790
Other	2	5.6250	0.1768	5.6250	.
Rand Merchant Bank	8	5.1250	1.6147	5.8750	-0.8340
Standard Bank	31	5.4516	1.4425	5.7500	-1.2120
Total	254	5.1004	1.4346	5.5	-0.692

The results related to whether the breach was preventable by the banking institution (controllability of cause) are negatively skewed across all demographic, and income groupings. This can be interpreted as respondents perceiving the data breach as preventable by the banking institution that announced it – see figure 5 below. This sentiment was consistent across most banks, except for a single respondent in Discovery bank, who perceived the breach as not preventable by the bank.

Figure 5: Histogram of the Perceived Controllability of Cause mean scores



5.6.4. Loyalty Intention

The dependant variable of loyalty intention was measured using a summed-scale with a 7-item rating scale. These values were computed from questions that sought to determine if a customer would act for or against the bank on matters related to word of mouth, switching intention and repeat patronage. The values were summed and averaged to generate an index, which was then used to generate table 16 below.

Table 16: Descriptive statistics for Customer Loyalty Intention

	N	Mean (M)	Std. Deviation	Median	Skewness
Total Sample	254	3.6839	1.7282	3.5000	0.319
Age					
18-24	3	3.7619	0.2182	3.7143	0.935
25-34	109	3.9345	1.8104	3.8571	0.138
35-44	88	3.4075	1.5982	3.0000	0.625
45-54	43	3.8040	1.7480	4.0000	0.134
55-64	11	2.9221	1.7431	2.0000	0.642
Gender					
Female	104	3.4684	1.7955	3.1429	0.606
Male	149	3.8380	1.6743	3.8571	0.121
Prefer not to say	1	3.1429	.	3.1429	.
Income					
R500 000 - R699 0000	82	3.6115	1.7019	3.5000	0.345
R700 000 - R899 000	67	3.5416	1.7207	3.5714	0.339
R900 000 - R1.1 Million	38	3.9023	1.7156	3.8571	0.015
more than R1.1 Million	67	3.7910	1.7935	3.1429	0.435

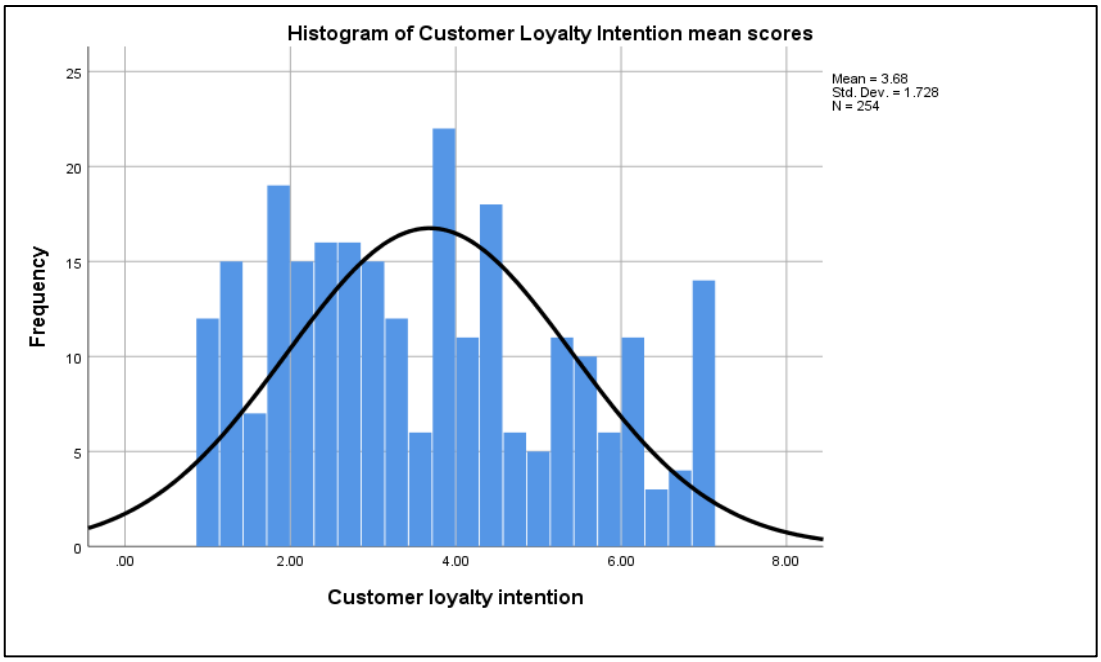
The data shows that customer loyalty intention is slightly positively skewed, although when plotted presenting as more normally distributed – see figure 6 below. That means customer loyalty intention tended to be more positive post the breach scenario.

Table 17: Descriptive statistics for Customer loyalty intention by group

Descriptives		Experiment Group					
		LS + IL	MS + IL	HS + IL	LS + EL	MS + EL	HS + EL
Mean		3,6891	3,6681	3,7546	3,7350	3,7946	3,5121
95% Confidence Interval for Mean	**Lower Bound**	3,1420	3,1050	3,1579	3,2591	3,2385	3,0146
	Upper Bound	4,2361	4,2312	4,3512	4,2110	4,3508	4,0097
5% Trimmed Mean		3,6401	3,6741	3,7273	3,7053	3,7530	3,4698
Median		3,6429	3,3571	4,0000	3,4286	3,6429	3,0000
Variance		2,458	2,604	3,388	3,513	2,379	3,259
Std. Deviation		1,56787	1,61384	1,84057	1,87424	1,54244	1,80515
Minimum		1,14	1,00	1,00	1,00	1,29	1,00
Maximum		7,00	6,29	7,00	7,00	7,00	7,00
Range		5,86	5,29	6,00	6,00	5,71	6,00
Interquartile Range		1,71	3,07	3,00	3,14	2,21	3,29
Skewness		0,831	0,101	0,119	0,331	0,365	0,382
Kurtosis		0,287	-1,182	-1,007	-1,075	-0,526	-1,122

The descriptive statistics by experiment group also show a slight positive skew. The skew, however, is more pronounced for the group Low Severity and Internal locus (LS + IS) with a skew statistic of 0.831. This may highlight that respondents that got a Low severity breach that was caused by a fault outside of the bank, tended to show more positive loyalty intentions than the other groups.

Figure 6: Histogram of Customer loyalty Intention Mean Scores



5.7. Results per Hypothesis

The main hypotheses tested all related to the impact of data breaches on customer loyalty intention. The key independent variables related to the customers perceived causes of the breach, which included the cause of the breach (internal or external), the likelihood of the breach re-occurring (stability of the breach) and whether the breach was preventable or not by the breached institution (Controllability of cause). These were tested against the dependent variable of customer loyalty intention, which is related to the customer performing repeat patronage, switching behaviours and word of mouth, which were measured by a single summed-scale referred to as customer loyalty intention. The final hypothesis related to the testing of breach severity and its impacts on loyalty intention. The analysis applied to hypothesis 1 and 4 will be similar as it considers the moderating effects of severity.

The results of the hypothesis testing are presented below.

5.7.1. Hypothesis One and Four: Locus of Causality and Data Breach Severity on Loyalty Intention

The null hypothesis related to the influence of the perceived locus of causality of a data breach and its impacts on customer loyalty intention, states that perceived external locus of causality (ELC) of the data breach will not have an impact on

customer loyalty (CL). The alternative hypothesis states that a perceived external locus of causality of the data breach will negatively an impact on customer loyalty (CL).

$H1_0$: $CL_{ELC} - CL = 0$

$H1_1$: $CL_{ELC} - CL > 0$

Since that hypothesis related to two independent categorical factors (locus of causality and breach severity) in line with the factorial design of the study and a single continuous response-dependent variable (customer loyalty), a two way ANOVA was utilised as an appropriate test. A two-way analysis of variance further referred to as a two-way ANOVA, is used to test the statistical significance of the means of two or more groups. Since the study was between subjects, we used a between-subjects/ independent ANOVA to assess the hypothesis. The table 18 below shows the results of the ANOVA conducted.

Table 18: Two-way Analysis of Variance

Tests of Between-Subjects Effects

Dependent Variable: Customer loyalty Intention

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta squared	Observed Power[b]
Corrected Model	2.323[a]	5	.465	.153	.979	.003	.085
Intercept	3256.409	1	3256.409	1072.097	.000	.812	1.000
Breach Severity	.443	2	.222	.073	.930	.001	.061
Locus of Causality	.032	1	.032	.011	.918	.000	.051
Breach Severity * Locus of Causality	1.540	2	.770	.254	.776	.002	.090
Error	753.280	248	3.037				
Total	4202.694	254					
Corrected Total	755.602	253					

a. R Squared = .003 (Adjusted R Squared = -.017)

b. Computed using alpha = ,05

Based on the above table 18, the results of the two way ANOVA show that there is no statistically significant effect of the independent variables of Breach Severity (sig = o.93 > 0.05) and Locus of Causality (sig = o.918 > 0.05) on the dependent variable of loyalty intentions. This is also true for the interaction effect of breach severity and

locus of causality, where there is not a statistically significant effect on customer loyalty (sig = 776 < 0.05). Despite this, the table does show that the interaction effects can explain 0.2% of the effect. Thus, we fail to reject the null hypothesis for $H1_0$ and $H4_0$.

We also note that the R-squared value also showed that only 0.17% of the variation in the dependent variable between the groups.

We now consider the tests for hypothesis two and three.

5.7.2. Hypothesis Two and Three: Perceived Stability of Breach and Perceived Controllability of Breach

The second null hypothesis related to the stability of cause states that customer perception of the breach conditions as stable with not impact customer loyalty to the organisation. It is summarised by the equation below

$H2_0$: $CL_{PS} - CL = 0$
$H2_1$: $CL_{PS} - CL > 0$

The third hypothesis related to the controllability of cause and it states that customer perception of the breached organisations control over the data breach will have no impact on their customer loyalty to the organisation. It is summarised by the hypothesis below:

$H3_0$: $CL_C - CL = 0$
$H3_1$: $CL_C - CL > 0$

To analyse hypothesis two (stability of cause) and three (controllability of cause), Structural Equation Modelling (SEM) was used, executed through IBM SPSS Amos. Structural equation modelling also referred to as causal modelling, is a technique that includes several types of analysis including path analysis, factor analysis, regression, simultaneous equations and others. It is especially useful for analysing interrelated measures relationships within a system and determining covariance between variables (Hair et al., 2007). To consider the full relationship, the secondary

measure of perceived Locus of causality (the measured locus of causality utilising summed-scales) were also included in the model, in order to determine any relationship between the variables of perceived stability of cause and perceived controllability of breach. The use of SEMs was supported based on similar usage by similar studies (DeWitt et al., 2008; Farah, 2017; Huang, 2008). As discussed in previous sections of the paper, the variables in the model were computed based on summed-scales.

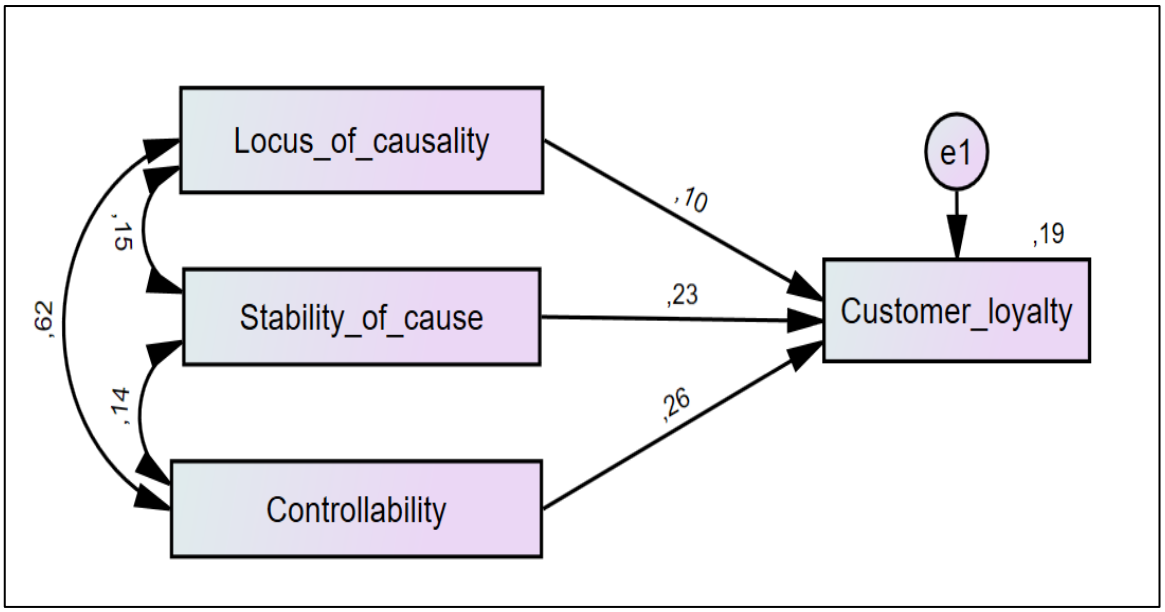
The Model of the hypothesised relationships was computed using IBM SPSS Amos 26. According to Huang (2008), structural equation modelling does not have a single measure to test model fit and thus several tests need to be applied which consider both the absolute and incremental model fit. In his study he utilised the Chi-squared goodness of fit (x2), root means square error of approximation (RMSEA), Normed Fit Index (NFI), Goodness of Fit Index (GFI). The results of the tests showed a good model fit, with only the RMSEA value being higher than the acceptable level of 0.08.

These results are summarised below:

- Chi-squared = 0 which should show 3 or less.
- RMSEA = 0.338 should be less than 0.08 for good fit
- GFI = 1 where a value of greater than 0.9 represents a good fit
- NFI = 1 where a value of greater than 0.9 represents a good fit
- CFI =1 where a value of greater than 0.9 represents a good fit

The structural model used to test hypothesis two and three are depicted in Figure 7 below as a Path Analysis. This figure also includes the path coefficients which will be used to interpret the results in Chapter six.

Figure 7: Structural model of hypothesis 2 and 3



The diagram above shows the observed exogenous variables of Locus of causality, the stability of cause and controllability of cause and the relationship between the observed endogenous variable of customer loyalty. The Covariances between locus of causality and Stability of cause, Locus of causality and controllability of cause and stability of cause and controllability of cause are also shown (β = 0.15, β = 0.62, β = 0.14, respectively). All the covariances are positive, highlighting that there is a positive link between the independent variables. In addition, the positive link between Locus of causality and controllably is much stronger at β=0.62, when compared to the other variables. The R-squared value of 0.19, shows how much variability in the dependent variable of customer loyalty can be explained by the three independent variables included in the model (19%).

Table 19 below shows that there is a statistically significant relationship between the perceived stability of the cause of the breach and customer loyalty intention with a P-value <0.001 i.e. the P-value is less than the significance value of 0.05 (β= 0.23, P<0,001. t= 4.05). This means we reject the null hypothesis $H2_0$, for the alternative hypothesis that stability of cause will negatively influence customer loyalty intention. That is, the more likely a customer views the breach as occurring in the future, the more likely they are to change their customer loyalty intention against the breached organisation.

Controllability of cause also shows a statistically significant relationship with customer loyalty with a P-value < 0.001 (β= 0.26, P<0,001, t= 3.55). This also means we reject the null hypothesis $H3_0$, for the alternate hypothesis that customer perception of the breached organisations control (C) over the data breach will negatively impact customer loyalty (CL) to the organisation. That is, the more a customer views the breach as preventable by the company, the more likely they will change customer loyalty intention against the breached organisation.

In addition, the relationship of perceived Locus of causality and customer loyalty does not have a significant relationship, with a P-value = 0.184 which is greater than 0.05 (P=0.184, t=1.32). This supports the results gathered in Hypothesis one ($H1_0$) that there is no significant evidence to reject the null hypothesis that locus of causality negatively impacts customer loyalty, and thus we fail to reject the null hypothesis.

Table 19: Structural Equation model results

			Estimate	S.E.	C.R.	P
Customer loyalty	<---	Locus of causality	,114	,086	1,328	,184
Customer loyalty	<---	Controllability	,311	,087	3,572	<,001
Customer loyalty	<---	Stability of cause	,262	,064	4,081	<,001

Table 20 below, further shows that there is a positive statistically significant relationship between the Perceived Locus of Causality and the perceived controllability of Cause (P<0.001). This will be discussed further in Chapter six.

Table 20: **Structural Equation model results: Covariance**

			Estimate	S.E.	C.R.	P
Controllability	<-->	Stability of cause	,320	,141	2,277	,023
Locus of causality	<-->	Stability of cause	,337	,143	2,358	,018
Locus of causality	<-->	Controllability	1,281	,154	8,340	<,001

5.8. Summary of findings

We conclude with a summary of the findings established through the chapter by presenting table 21 which provides an overleaf of the hypothesis testing.

Table 21: Summary of Hypothesis testing results

Hypothesis	Fail or Reject the null hypothesis
$H1_0$: Perceived external locus of causality (ELC) of the data breach will not have an impact on customer loyalty (CL)	Fail to reject $H1_0$
$H2_0$: Customer perception of the breach conditions as stable with not impact customer loyalty to the organisation.	Reject $H2_0$
$H3_0$: customer perception of the breached organisations control over the data breach will have no impact on their customer loyalty to the organisation.	Reject $H3_0$
$H4_0$: Data breach severity (DBS) does not influence the relationship between perceived locus of causality (LC) and customer loyalty (CL)	Fail to reject $H4_0$

Chapter 6: Discussion of Results

6.1. Introduction

This chapter aims to provide the interpretation of the results from the previous chapter. The results are discussed, and insights that can be derived disclosed.

The Chapter six will therefore examine in detail, the primary research questions as they were presented in Chapter two and Chapter three. The section aims to show how the analysis insights answer the fundamental question of the study; “what is the impact of data breaches of varying severity on customer loyalty?”. Insights will be provided as well as an assessment of these results, against the current literature and theories presented in the earlier parts of the paper.

6.2. Demographic and descriptive statistics

The study begins by discussing the demographic and descriptive statistics of the respondents in the study. A total of 254 respondents completed the survey and met the sample frame of a minimum age of 18, an annual income above R500 000 and a valid and active South African bank account. The sample was gathered through a survey questionnaire, where one of six data breach scenarios was randomly assigned to a respondent. These scenarios highlighted the varying levels of severity and causes (locus of causality) as defined in the methodology. Based on the tests that were performed, the sample size was deemed sufficiently large to conduct meaningful statistical analysis (Aguinis & Bradley, 2014; Vanvoorhis & Morgan, 2007). The statistical analysis was mainly executed through the ANOVA, T-test and Structural Equation Modelling. While the survey was distributed to a wide group of individuals, several biases were noted which will be elaborated on below.

The sample showed a slight bias of males (59%) compared to females (41%). This bias also remained relatively consistent across the six groups of respondents and can be explained by the income criterion for the study, where the income differential between males and females is anecdotally skewed more in favour of males. Men have historically earned a higher salary than females both in South Africa and Globally (Ortiz-Ospina, Esteban Roser, 2019). However, while there were slight

differences in the gender composition of the study, gender was not a variable that was critically assessed in the study.

The age profile of respondents was listed at 1% in age group 18-24, 43% in group 25-34, 35% in 35-44, 17% in 45-54 and 4% in 55-64%. No respondents were reported in the age group 65+. This age profile is in line with the employed age population of South Africa, where ages 25-34 represent the second largest population of economically active South Africans (Stats SA, 2020). When assessing this against the literature, Ngobo (2017) states that true customer loyalty may change and vary based on a customer's age. The statistical analysis conducted in this study contradict this view with preliminary results indicating that loyalty intention across the age intervals remained relatively stable across the groups. This means that age alone was not a big driver of loyalty. In a similar study by Choi, Kim and Jiang (2016), focusing on the impacts of recovery efforts on customer behaviour, it was also determined that age did not have a statistically significant impact word of mouth, switching behaviour and repeat patronage, which supports the findings in our study, and contradicts the findings from the research conducted by Ngobo (2017).

In the study, another key statistic related to financial means, proxied through the annual income of respondents. Respondents, who presented an annual income of less than R500 000 were excluded from the study. This was in line with the sample frame defined in Chapter four. Financial means were identified by Pick and Eisend (2014), as one of the key barriers to switching once customers had experienced a negative event, like a data breach. Switching behaviour was identified in the literature as the most significant trait of customer loyalty following a negative experience (Pick & Eisend, 2014) and thus, limiting the eligibility of respondents with sufficient financial means, meant the study would aim to better understand the true behaviour intention of customers following a data breach i.e. if money was not a barrier, would the customer have remained loyal to the banking institution following a data breach? This literature was used to support the choice in the sampling frame for the study.

The income variable showed a slight bias towards income group R500 000 – R699 000, with 32% of respondents falling within this category. This income group is considered as the entry-level income band into Private Banking when compared to others. These clients may not possess the financial means, and thus the same ability

to change their intention as those who earn a higher annual income. However, the descriptive statistics showed that the average loyalty intention (M=3.6) and skewness (0.345) aligned with that of the other income groups, reducing the perceived impacts of income in biasing the study.

The sample also highlighted a consistent skew towards a single bank across the cell groups measured. First National Bank represented 58% of the sample as the primary banking institution for respondents of the study. Standard Bank, ABSA, Investec and Capitec Bank represented the remainder of participants with 12%, 9%, 7% and 6% respectively. This skew in the banking institution demographic towards a single bank can be explained by the data gathering process followed. The introduction of a boosted sample, which was predominately distributed to FNB employees, meant that the sample would inherently be biased towards the bank. Further analysis of the data showed that while this was consistent across the six groups, it resulted in no statistically significant impact on the dependent variable namely, customer loyalty intention, when compared to the first sample. The t-test concluded that the two independent samples were drawn from the same population (P= 0.249, t=1.15). This said, any bias resulting from sentiments towards the employer for respondents in the boosted sample cannot be fully accounted for in the study.

Factors like employee sentiment towards the organisation could skew results of loyalty intentions both for and against the employee's organisation. Literature also supports this view that employee attachment can lead to loyalty, emotional attachments and feelings of obligation to the organisation (Shah, Irani, & Sharif, 2017). These can be maintained even despite challenges like organisational change or in this case, data breaches in the organisation (Shah et al., 2017). This attachment can then lead to maintained loyalty irrespective of challenges. This provides an alternative explanation for the loyalty of staff following a data breach. Specifically for retail banking, long term relationships with specific employees was also found to sustain positive loyalty intentions by acting as a barrier to loyalty changes like switching (Beerli et al., 2004). These were determined to be difficult to overcome, despite dissatisfaction from customers.

Despite these biases, the sample data was considered usable for the study, with Cronbach's alpha used to confirm the reliability and quality of the scales used. Results showed, like in other studies that the scales were reliable.

6.2.1. Customer Loyalty Intention

Customer loyalty, in this study, is the measure in which customers express their likelihood of displaying intentions across a combination of metrics including word of mouth, repeat patronage and switching behaviour (Watson et al., 2015). Across various demographics and samples, the customer loyalty intention in the results of the study tended to show a very slight positive skew (0,319), with summed-scale means showing that customers displayed a more positive to neutral loyalty intention despite the data breach (M=3.68). Furthermore, those that considered the breach as low in severity and not as a result of the bank's actions (or lack of actions) during the scenario's (group 1 LS + IL), tended to display more positive loyalty intentions than other groups. This is evidenced by the larger positive skew (0.831) of the mean average scores (M=3.68).

This is explained and supported by the defensive attributions theory, which explains that the less severe a breach is, the less compelled a customer would need to attribute blame for its cause (Zhou & Ki, 2018). For the study and this specific group that viewed the low severity internal locus scenario, this supports the theory i.e. the severity of the cause was low, which then led to a smaller need to allocate blame, thus resulting in a less negative loyalty response. In addition, the consequences of accepting blame for the cause of the breach may have also been viewed as insignificant by respondents from a severity perspective – thus making it easier to maintain a positive loyalty position. This is also further strengthened by the vignette scenario which suggests that the breach was caused by the direct actions of the respondent and thus attribution of blame would have been more likely directed towards the individual themselves in the form of self-blame. However, the other groups did not align to the defensive attribution theory and literature, and rather reflected a stable positive loyalty intention despite variations in severity and locus of causality – see Table 17 above for full details. This divergence from the expected literature is discussed next and further in the hypothesis testing of the experiment.

There are some concerns that other factors outside of breach cause may have impacted the general sentiment by respondents related to customer loyalty. Watson et al. (2015), states that loyalty behaviours like switching are also influenced by psychological factors – like one's sentiments about the assessed organisation or previous experiences. Customers who may have had a positive experience with a supplier before the negative event may find it difficult to switch despite negative events (Watson et al., 2015). That is, customers may have had positive experiences with the breached banking institution and been less likely to change loyalty behaviours based on a single breach and level of severity. This is also supported by the questions posed in the study about the respondent's previous breach experience, with 62% of respondents reported as never having experienced a data breach.

This would indicate that this breach scenario would have been the first time they had been presented with a data breach related to their institution. This may suggest further areas of investigation in future studies to further unpack. This said, customer loyalty refers to an ongoing relationship between a supplier and its customers and thus may need to be measured over a period rather than a point in time study. This will be discussed under future considerations in chapter seven.

To summarise, despite this potential bias and concerns, the testing of the measurement instruments based on Cronbach's Alpha, suggested that they were reliable and could be used in the study.

6.3. Hypothesis 1 and 4. Locus of Causality and Breach Severity of Customer Loyalty Intention

We now discuss the results of Hypothesis one and four, which were concerned with testing the impact of the locus of causality and the breach severity on customer loyalty intention. As these hypotheses were tested using the same two-way analysis of variance (ANOVA), to determine if there were any statistically significant differences between the six groups presented with varying levels of breach severity and causes of the breach, they will be discussed under the same section for ease of reference.

6.3.1. Hypothesis 1 – Locus of Causality on Customer Loyalty

The objective for hypothesis one was to understand if an external locus of causality would negatively impact the customer loyalty of banking clients. Specifically, would a breach that was by all accounts caused by the breached organisation lead the customer to change their loyalty intentions to be against the breached organisation. The null hypothesis stated that the locus of causality would have no impact on the customer loyalty of banked clients. This hypothesis was derived by reviewing previous in the literature and studies, which supported the view that a data breach would be considered by respondents as being caused by an external factor, and would lead to reduced future purchase commitments against the organisation (Goode et al., 2017; Martin & Murphy, 2017). Thus, the alternate hypothesis presented as; a perceived external locus of causality of the data breach would negatively impact on customer loyalty.

The use of descriptions like “employee negligence” and “customer device” in the randomly assigned vignettes, was designed to differentiate the cause of the breach to be either external (the bank) or internal (the customer) in nature. These descriptions proved to be clear during pilot testing. However, when compared against a complementary set of measures designed to test how the customer understood the cause of the breach – it was established that the majority of customers saw the breach as external in nature despite the vignette explicitly highlighting the cause otherwise (M= 5.4). This phenomenon can be explained by Werner (1985), where he found that individuals have a tendency to apportion blame for the causes of negative events to external factors and causes of positive outcomes to their own actions - Hedonic bias. This would then lead respondents to apportion the blame of the breach in the study to the bank, classifying it as an external locus of causality.

The results of the hypothesis testing failed to reject this null hypothesis, that the locus of causality has no impact on customer loyalty intention. While this view at first seems to contradict current literature presented. The secondary complementary measure used for the perceived locus of causality, derived through summed scales, provides some insight into why. In line with previous studies, most customers tended to have evaluated the impact of the breach cause as external in nature and did not differentiate this view despite some vignette presenting an internal cause of the

breach (Weiner, 2001). This supported the theory that customers tended to associate negative events with an external locus of cause and once data has been exchanged, they shift responsibility to the external provider – in this case the breached institution (Martin & Murphy, 2017). Monroe and Lane (2019), further support this, by stating that most people first pass judgement based on perceptions and social norms, before evaluating the facts and the details of the negative event. While the shift to affirm blame as a result of the external party is in line with the literature, the lack of change in customer loyalty intention is not.

The literature suggested that if the locus is perceived as external in nature, customers would display lower loyalty intention and willingness to repurchase from that company (Pick et al., 2016). Our results contradict this view. Moreover, the subsequent loyalty response once the locus had been affirmed as external in nature, remained relatively positive/neutral and not against the organisation. Sayani (2015), explains that despite sentiments of switching, customers may remain loyal to the bank due to the high perceived switching barriers related to the banking industry. This consideration supports the fearful and secure styles of attachment theory, where customers that trust the bank or fear leaving the bank, fail to act against the bank through loyalty changes, despite a product harm crisis like a data breach, due to their positive affiliations to the institution (Whelan & Dawar, 2016). This may give insight that customers, despite seeing the cause because of the bank's actions, remained loyal due to the perceived consequences of reducing loyalty intention. It is suggested that this needs further study to be affirmed or rejected.

Thus, the studies aspiration to prove that an external locus of causality has a negative impact on customer loyalty could not be upheld based.

6.3.2. Hypothesis Four – Data Breach Severity

The objective of hypothesis four was to determine the impact of breach severity on customer loyalty, by evaluating the moderating impacts of breach severity on the relationship between the perceived locus of causality and customer loyalty intention. According to Aivazpour, Valecha, Chakraborty (2018), it is argued that customers do not value information the same, but rather evaluate it based on the perceived risk it posed. Moreover, using Defensive Attribution Theory, it is also argued that the more

severe the negative outcome, the stronger the need to attribute responsibility to the cause of the outcome to an external locus of causality (Zhou & Ki, 2018). That is, the severity of the risk posed by the information included in a data breach was hypothesised to worsen the customer's loyalty response to the announcement of a data breach and further increase the blame placed on the organisation. Thus, we hypothesised that data breach severity would negatively influence the relationship between perceived locus of causality and customer loyalty intention.

The framing of severity in the vignettes was determined using a data breach index, which incorporated factors like size, type and potential of harm to customers, to derive a severity grouping that would be classified as either High, Medium or Low based on the specified values (Stiennon, 2013). The theory suggested that customers would be more likely display enhanced negative loyalty intentions due to the enhanced the attribution of blame towards the organisation, driven by the severity of the breach (Zhou & Ki, 2018). Based on this, the null hypothesis then stated that data breach severity does not influence the relationship between perceived locus of causality and customer loyalty.

The results of the Two-way ANOVA used to test the hypothesis, as seen in table 18 above, determined that there was not a statistically significant relationship between the individual and combined factors in determining changes in customer loyalty intention. Thus, we failed to reject the null hypothesis that breach severity does not influence the relationship between perceived locus of causality and customer loyalty. The two independent factors of breach severity and locus of causality did not adequately explain the changes in the dependent variable of customer loyalty intention, with only 0.17% of variation explained. This goes against previous literature, that had found that severity impacted organisation and customer response to service failures, like data breaches (Malhotra & Malhotra, 2011). This suggests that unlike the impacts at a firm level (Malhotra & Malhotra, 2011), severity plays a smaller role in customer determining changes in customer loyalty intention post a data breach.

Again, we refer to Blut et al. (2015) to explain the possible reason for this departure from the literature. By only associating the blame as being external in nature, customers do not then amend their loyalty intention to be against the breached

organisation. Further considerations possibly related to ease of switching like the number of competitors, switching costs and barriers, and emotional commitment to the organisation tend to also influence the loyalty intentions of customers (Blut et al., 2015).

6.4. Hypothesis 2 and 3 – Stability and controllability of Cause

We now consider hypothesis two and three, which are concerned with the customer perception of the likelihood of a data breach reoccurring in the future at the breached organisation (stability of cause) and whether the breach was preventable by the breached organisation (controllability of cause). Both these hypotheses were tested using structural equation modelling to capture the causal relationship, if any, related to these constructs and to determine if there were statistically significant relationships between the constructs.

6.4.1. Hypothesis 2 – Perceived Stability of Cause.

The second hypothesis related to the perceived stability of the cause of the data breach, and the likelihood of the breach reoccurring in the future. Theory suggests that customers will assess the likelihood of the breach occurring in the future and will then make decisions to guard against future harm by amending loyalty intention about the company (Goode et al., 2017).

Furthermore, psychological response evaluation, explains that breaches in customer information will increase a customer's view of potential future harm, and will lead to the customer taking precautionary measures to prevent future harm (Choi et al., 2016). And thus, we hypothesised that an enhanced perception that the breach was likely to occur in the future, would negatively impact customer loyalty. That is, customer perception of the breach conditions as stable will negatively an impact on customer loyalty.

The hypothesis was tested using structural equation modelling, and the results as summarised in table 19 above, showed that there was a statistically significant positive relationship between the perceived stability of the cause and the loyalty intention of customers ($\beta = 0.23$, $P<0{,}001$. $t = 4.05$). That is, there was a positive

correlation between the likelihood of reoccurrence of the breach in the future and the negative loyalty response by customers. thus, we reject the null hypothesis for the alternate hypothesis.

These results support the current literature that customers will reduce their loyalty towards a breached organisation if they perceive that there is a high likelihood of the breach occurring again the future (Choi et al., 2016). It is further stated that organisations must take the necessary steps to guard against adverse loyalty outcomes (Choi et al., 2016). This could suggest some implications for organisations that in announcing a data breach, it may be in the organisations best interest to assure customers that the likelihood of the breach reoccurring in future remains low. This can be achieved by showcasing the different steps that have been taken to address the breach by the organisation and in line with the finding of hypothesis one of the study, this should be done despite the true cause of the breach being outside of the company's direct control. We will elaborate on this potential implication further in Chapter seven.

6.4.2. Hypothesis 3 – Perceived Controllability of Cause.

Hypothesis three addresses the dimension of perceived controllability of the cause and seeks to determine the impact on customer loyalty of a perception that the breach was preventable by the breached organisation.

According to attribution theory, customers apportion blame by considering the perceived control of the cause of a negative outcome like a data breach (Pick et al., 2016). That is, customers will determine blame and subsequent response to a data breach by considering the level of control the organisation had in preventing the negative outcome. We hypothesised that customer perception of their control of the data breach will increase or maintain customer loyalty to the organisation. Simply put, a customer's perception of the level of control they had in preventing the data breach would influence their loyalty intention to the organisation. The null hypothesis was then stated as customer perception of their control of the data breach will have no impact on their customer loyalty.

This hypothesis was tested using a structural equation model, where results in table 19 above, show that there is a statistically significant relationship between the perceived controllability of the breach and the customer loyalty intention of customers (β= 0.26, P<0,001, t= 3.55). thus, we rejected the null hypothesis for the alternate hypothesis as stated above. Furthermore, there was a positive relationship between perceived controllability and loyalty intention, which suggests that customers that viewed the breach as preventable by the breached organisation, tended to change their loyalty intention to be against the organisation post the breach. This result supports the theory that customer control over their data, and by extension, the ability to prevent harm, suppresses their feelings of vulnerability during a negative scenario, which in turn suppresses the need to act against the organisation to prevent future harm (Martin & Murphy, 2017).

In addition, the results of the study support the results established by the motivated blame models. These models found that blame is reduced when the cause of the negative event is considered unintentional (Monroe & Lane, 2019). This provides further insight.

In general, customers tended to perceive the controllability of the cause of the breach as being preventable by the breached organisation (mean average score = 5.1, skewness = -.692). This was across all demographic factors considered in the study (age, gender, income, primary banking institution). This supports the theory that in most instances perceived controllability is a subjective measure, and less objective (Skinner, 1996). In addition, research suggests that customers expect organisations to take measures to secure their personal information and prevent future harm (Goode et al., 2017). It has been established that data protection thus can be seen as part of the service offering of the organisation, and by extension in the direct control of the organisation (Malhotra & Malhotra, 2011). Thus, a failure to fulfil this service is deemed as preventable by customers i.e. controllable by the organisation. Supporting this finding of the study.

The study also found a statistically significant link between the perceived locus of causality and perceived controllability of cause (P<0.001) in explaining the impact of breach severity on customer loyalty intention. This positive relationship (β=0.62), suggests that there is a link between how blame is apportioned, where consideration

around the cause of the breach being internal or external in nature is given, then permutates into consideration related to whether the breach was preventable by the organisation. This can also be viewed as customers blaming the organisation for the breach (external locus) because it was preventable. This finding supports the literature by Munyon, Jenkins and Crook et al. (2019), who cite that the locus of causality and the controllability of the cause are the most important dimensions in assigning judgement and responsibility for an event. Moreover, they state that the combination of these dimensions determines about is responsible and whether the negative results could have been avoided (Munyon et al., 2019), are the key determinants of passing judgement and responsibility. This highlights that customers view the interaction of the two dimensions as necessary for passing blame.

Linking this to the findings determined under hypothesis one, we see that in general, customers tend to associate the cause of negative events to an external factor, in this case, the breached organisation, despite evidence suggesting alternative causes. Kashmiri et al. (2017) then further suggests that blame for the privacy breach is then placed towards senior managers of the breached organisation, as they are perceived to control the factors to prevent the privacy breach (investments into data privacy infrastructure). This then gives insight that customers that already see the breach as being caused by an external factor are also going to see the breach as preventable by members of the organisation (controllability of the cause), thus explaining the strong link between locus of causality and controllability of cause established in the study.

6.5. Summary of Discussion

The discussions above have established several key findings within the study about the impact of data breaches on customer loyalty intention, which will be summarised below.

Of the hypothesis tested, it was determined that the locus of causality and data breach severity did not significantly influence or explain the changes in customer loyalty post a data breach, contradicting what was initially expected from the literature reviewed. While this does not fully support the literature investigated, elements related to how customers perceive the breach aligned.

Key to this insight was the confirmation that most customers would associate negative news with an external locus regardless of the scenario or facts presented due to their bias to associate negative news with the breached company. Attachment theory literature may give insight into why customers remain with positive loyalty intentions post the negative sentiment, but this is not fully captured and will need further investigation. Some concerns are also raised by the findings of the study around other factors that may have resulted in customers maintaining loyalty intention despite this fact agree that the cause was related to the breached company. Factors including previous loyalty standing with the organisation, previous experiences with the organisation and the switching barriers associated with the Banking industry, are all factors that could have prevented loyalty changes against the company in line with literature cited (Blut et al., 2015). These will be raised for consideration in future studies.

The second and third propositions, related to stability and controllability of breach and proved to be statistically significant.

On stability, the hypothesis supported the presented literature that customer loyalty intention is impacted by the likelihood of the breach occurring again in future. Furthermore, it supported the notion that customers who believed the breach had a high likelihood of re-occurring would protect themselves against future harm by decreasing their loyalty intention towards the organisation (Goode et al., 2017). In our discussion we also sight that accountability and addressing what the organisation can do prevent future breaches, may position the organisation in a better light in dealing with the breach.

On Controllability of the cause, the hypothesis supported the literature that customer loyalty intention is impacted by the perceived control that an organisation had in preventing the breach. This was supported by the theory presented in the literature review, implying that an adverse loyalty response would occur as a result of the organisation being perceived to have had the ability to prevent the breach. The key take-out being that this is a subjective view that needs to be recognised by the organisation consumers may not be privy to the true privacy structures of the organisation.

A further insight that was obtained through the results was the statistically significant link between the controllability of the breach and the locus of causality. Customers who tend to already view the breach as caused by an external factor (the organisation) also then compound this view by interpreting the breach as preventable by that external factor. This follows based on the expectation by customers that it is the organisation's role to have infrastructure and policies to protect their data, and thus a breach that is generally perceived to be the organisations doing will result in blame evident through changes in customer loyalty intention.

Lastly, we conclude this section by relating the above discussions to the initial objectives presented for the study in chapter three.

Objective 1: was to determine how the causal inference factors of Locus of causality, stability and controllability, influence customer loyalty post a data breach for high net-worth clients in retail banking. Based on the results and discussion, this study has found that there is a statistically significant relationship between the factors of stability and customer loyalty, and controllability of cause and customer loyalty. However, evidence from the study shows that there is no statistically significant relationship between the locus of causality and customer loyalty, but a new relationship exists between the locus of causality and the controllability of the breach.

Objective 2: was related to understanding the role of breach severity in influencing the relationship between the factors identified in objective one and the customer loyalty of high net worth clients, by presenting six differing breach scenarios controlled for breach severity. Do customers respond differently to data breaches of varying severity?

The study found that there was no statistically significant relationship between breach severity in explaining changes in customer loyalty intention, which contradicts reviewed literature.

Chapter 7: Conclusion and Recommendations

In this final chapter, the key findings, theoretical implications, and the implications for organisations and academics alike, will be discussed. We then conclude the chapter with limitations and proposals for future areas of research related to the study.

7.1. Introduction

The study set out to understand the impact of data breaches of varying severity on customer loyalty. High net worth banking clients were selected as the population under study to best illustrate the this impact with in the banking industry as they had both the means and the ability to change, their loyalty intentions despite the perceived switching barriers associated with the industry. This was identified in the literature as critical for assessing loyalty intentions of customers post a data breach event. Furthermore, the study sought to extend to the academic body of literature using constructs from attribution theory to determine the causal relationship of how customers allocate blame post a data breach and the subsequent impact on customer loyalty. This produced mixed results when compared to the literature assessed, and the principal conclusions are discussed below.

7.2. Principal conclusions

From a theoretical perspective, the study intended to extend the use of attribution theory and its constructs to determine how customers assign blame during negative events, through changes in their loyalty behaviour. Literature suggests that understanding this at a micro-level (the customer) has been limited (Aivazpour et al., 2018; Munyon et al., 2019), and the thus study has extended to this body of knowledge through the following theoretical propositions and findings.

Our first finding confirmed that customers tend to observe the cause of a data breach as being a result of an external factor over their own actions. This is despite objective details suggesting that the underlying cause is a result of the customer's actions. This bias, identified in the literature as the hedonic bias (Weiner, 1985), is confirmed as prevalent in the study across the majority of respondents sampled. This also supports the literature that blame for negative events is subjective and based on

perception, over objective reasoning. Customers respond based on perception and then attempt to justify their reasoning using facts that support their argument (Monroe & Lane, 2019). Importantly, while there was broad acceptance by participants in the study that the locus of cause of the breach is perceived as external in nature, the study found that the locus of causality alone does not sufficiently explain the impact of the data breach on customer loyalty intention. Our findings show that there is no statistically significant relationship between the locus of causality and customer loyalty intention post a data breach.

However, that said, the locus of causality does combine with the controllability dimension of attribution theory to explain some responses in customer loyalty intention. The study findings support the literature that blame and judgement after a negative event is primarily passed after considering the combination of both elements regarding who caused the breach (locus of cause) and whether the breach could have been prevented from occurring (controllability of cause) (Munyon et al., 2019). This co-dependence between the two constructs suggests that they should be considered in tandem when assessing the potential impact of the breach by the organisations and academia.

Our second key finding relates to the stability of cause, which is the customers perceived likelihood of a breach occurring in future. Our findings supported the current literature that as part of the psychological response by customers for evaluating the level of blame to allocate for a data breach, customers would consider the likelihood of the breach re-occurring in future (stability) in determining blame, and would take the necessary steps to prevent any potential future harm by changing their loyalty intention towards the company (Choi et al., 2016).

The third finding relates to the controllability of the cause of the data breach, which refers to the level of control an organisation had in preventing the outcome. The findings of the study determined that there was a statistically significant relationship between the perceived controllability of the cause of the breach and the subsequent changes in loyalty intention. This was supported by the current literature that customers apportion blame by considering the perceived control of the cause of a negative outcome (Pick et al., 2016). Furthermore, this relationship is positive in nature, meaning that an increase in the perceived view that the organisation could

have prevented the data breach, will diminish customer loyalty intentions. That is, customers will more likely increase negative loyalty intentions against the company. Literature supports this relationship and explains it using the motivated blame models. Blame is reduced when customers find the cause of a negative event, like a data breach, when viewed as unintentional, and increased when viewed as intentional or preventable (Monroe & Lane, 2019). In the study this presented as the strongest of the relationships considered as impacting customer loyalty, aligning with previous findings that controllability of case is an important construct in determining blame (Munyon et al., 2019).

Our last key finding addresses the moderating impacts of data breaches severity on customer loyalty. Literature suggested that breaches of varying severity would have varying impacts on customer loyalty, and elements related to the perception of the causes of the breach (Aivazpour et al., 2018; Song et al., 2016). While literature was scant on breach severity, findings related to the impacts of severity at an organisational level had suggested that varying severity of breaches would impact customers differently (Malhotra & Malhotra, 2011). The results of the study contradict this view and found that breach severity did not sufficiently impact customer loyalty or the relationship between customer loyalty and locus of causality. The study found that it was only in one experiment group where severity was presented as low and locus of causality was presented as internal that there were small loyalty changes. These were explained by the literature through the defensive attributions theory, which suggests that the less severe a breach is, the less compelled a customer would need to attribute blame for its cause (Zhou & Ki, 2018). However, this theory did not support the remaining 5 groups of experiment results. Thus, the results show a weak relationship between breach severity, locus of causality and customer loyalty, which is not statistically significant.

To conclude, our findings extend to the literature related to attributions of negative events, especially at a micro-level. It also extends the understanding of data breaches on customer loyalty intentions by exploring the loyalty response of customers after the announcement of a data breach.

7.3. Implications and recommendations for managers and business

Previous literature has found that the prevalence of data breaches introduces significant impacts on organisations and their customers (Martin et al., 2017; Martin & Murphy, 2017). We now discuss the implications of this study to managers, marketers and business drawing from the key findings and results of the study.

For business, the importance of maintaining customer loyalty during and post a data breach is cited as being key to maintain long-term profitability (Chen, 2015; Janakiraman et al., 2018; Ngobo, 2017; Sayani, 2015). Sayani (2015) then further states, that this is heightened in an industry like banking, where the loss in wealthier customers can severely impact the profits of banking institutions. For managers, the literature also suggests that responsibility for the breach is often placed mostly on them as they are perceived to control the resources and means to prevent data breaches (Kashmiri et al., 2017). Janakiraman, Lim and Rishika (2018), further states that managers need to actively manage data breaches to preserve customer relationships. This is said especially true in retail banking where long standing customer relationships tend to act as barriers for adverse loyalty intentions like switching behaviour, despite negative incidents (Beerli et al., 2004). Based on our results we discuss implications for both groups of stakeholders and recommend the following suggestions.

Customers perceive the cause of the breach as external in nature i.e. caused by the actions of the breached organisation, despite some breaches presenting as being caused by actions of the customer. However, this determination will not in isolation, impact the loyalty intentions of customers. Furthermore, our findings suggest that customers will evaluate loyalty intentions by considering the potential for future harm and assessing the likelihood of the breach reoccurring in the future (stability of the cause of the breach).

The study's results suggest that managers should consider the manner in which customers will determine blame to positively impact or maintain customer loyalty. We recommend that managers and organisations should acknowledge their responsibility in causing the data breach (locus of cause) when announcing it to customers. This will not change customer loyalty intentions negatively and may

assist companies in regaining trust with their customers, which is often lost during data breach announcements (Choi et al., 2016). Restoring the trust relationship is critical in responding to a data breach (Choi et al., 2016). In addition to this, managers need to clearly articulate the steps taken to prevent the privacy breach from occurring in future, based on the resources available to the organisation. This, to persuade customers that the likelihood of the breach reoccurring in future (stability of cause) has been reduced, which is expected to improve customer loyalty towards the company.

The study found that another key dimension to be addressed post a data breach is the level of control an organisation, or customer has in preventing the data breach from occurring. Theory suggests that blame is reduced when the cause of the negative event is considered unintentional and not preventable (Monroe & Lane, 2019). Furthermore, the literature suggests that customer expect organisations to use their means to protect their data as part of the service they offer (Malhotra & Malhotra, 2011). Based on this and the study findings, managers should showcase all the controls implemented to prevent the breach. This should be done despite those supplementary controls given to customers to further protect their data.

Lastly, these actions should be considered despite the severity of the data breach, as the study suggests that customer loyalty intentions are not changed based on the breach severity.

7.4. Limitations of the study

This section discusses the limitations identified in this body of research.

The research was conducted using an experimental factorial design which is often criticised for the lack of generalizability of results (Aguinis & Bradley, 2014). This was partially addressed by making the breach more scenarios realistic and in line with a real-world breach scenario's, considering the work of previous studies and increasing the minimum sample size, as suggested by Aguinis and Bradley (2014). Despite these actions taken, this still may not completely address these concerns regarding experiments and thus is noted as a possible limitation for the study.

The way data was collected may also present a limitation to the study. The data was collected in two rounds of survey distributions, with the second round discussed in chapter four and five, as a boosted sample of employees who held accounts with the employer institution. This institution (First National Bank) also represented 58% of total respondents. While statistical tested reflected no significant impact of this to the study, the over-representation of one institution and the potential bias of the employer-employee relationship is identified as a limitation of the study.

A further limitation of the study results from the study utilising only a single method of data collection– survey responses. A combination of secondary data and face to face interviews can be considered to triangulate outcomes and strengthen the insights collected. We note this as a limitation of the study.

Lastly, the study was conducted at a point in time, however, a breach event forms part of the ongoing relationship between the breached organisation and the customer. Thus, the study may not have captured the full impacts of the data breach on the loyalty intentions of customers as it was conducted over too short a period. To support this view, some of the factors that impact loyalty intention occur overtime i.e. positive experiences and repeat purchases (Watson et al., 2015). These may be better assessed over a period and are presented as limitations for the study.

7.5. Recommendations for future research

The impact of data breaches on customers continues to remain topical due to their prevalence across different industries and organisations (Abratt & Russell, 1999; Jung et al., 2017; Kashmiri et al., 2017; Ngobo, 2017; Sen & Borle, 2015b). Using the lens of attribution theory to understand the causal relationship that exists between loyalty intention and the dimensions of attribution theory, the results of the study have been mixed, supporting the literature for dimensions related to stability and controllability of cause, while contradicting the literature for constructs related to breach severity and locus of causality. This leaves an opportunity for future research.

Post this study, future research can consider extending on the study by conducting a repeated measures study to address some limitations cited in section 1.4 of chapter seven. Respondents assessments of the breach scenarios can be evaluated

repeatedly over several months to better isolate the impacts of data breaches of varying severity on loyalty intention. The sample for the survey can also be extended more broadly to ensure results gathered are diverse more reflective of the complete population of study. Further research can be conducted using interviews to gather insights into data breaches and the responses by customers to their announcement.

Furthermore, due to its varying impacts on customer behaviour, there remains a lot to be understood about the impact of data breaches on customer behaviour as reflected by this study and others before it (Goode et al., 2017; Janakiraman et al., 2018). Future research can also consider the impact of breaches within other industries which present fewer switching barriers, and are more susceptible to loyalty changes (Kashmiri et al., 2017).

References

Abratt, R., & Russell, J. (1999). Relationship marketing in private banking in South Africa. *International Journal of Bank Marketing*, 17(1), 5–19. Retrieved from https://doi.org/10.1108/02652329910254000

Aguinis, H., & Bradley, K. J. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods*, 17(4), 351–371. Retrieved from https://doi.org/10.1177/1094428114547952

Aivazpour, Z., Valecha, R., & Chakraborty, R. (2018). The impact of data breach severity on post-breach online shopping intention. *International Conference on Information Systems 2018, ICIS 2018*, (July), 0–9.

Azorín, J. M., & Cameron, R. (2010). The application of mixed methods in organisational research: A literature review. *Electronic Journal of Business Research Methods*, 8(2), 95–105.

Barge, M. (2014). A METHOD FOR CONSTRUCTING LIKERT SCALES. *SSRN Electronic Journal*, 1–12. Retrieved from https://doi.org/10.1017/S0143385700004491

Beerli, A., Martin, J. D., & Quintana, A. (2004). A model of customer loyalty in the retail banking market. *European Journal of Marketing*, 38(1), 253–275. Retrieved from https://doi.org/10.5267/j.ac.2016.8.002

Blut, M., Frennea, C. M., Mittal, V., & Mothersbaugh, D. L. (2015). How Procedural, Financial and Relational Switching Costs Affect Customer Satisfaction, Repurchase Intentions, and Repurchase Behavior: A Meta-Analysis Abstract. *International Journal of Research in Marketing*, 32(2), 226–229.

Bonett, D. G., & Wright, T. A. (2015). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*, 36(1), 3–15. Retrieved from https://doi.org/10.1002/job.1960

Casadesus-Masanell, R., & Hervas-Drane, A. (2015). Competing with Privacy. *Management Science*, 61(1), 229–246. Retrieved from https://doi.org/10.2139/ssrn.2273006

Chen, S. C. (2015). Customer value and customer loyalty: Is competition a missing link? *Journal of Retailing and Consumer Services*, 22(July), 107–116. Retrieved from https://doi.org/10.1016/j.jretconser.2014.10.007

Choi, B. C. F., Kim, S. S., & Jiang, Z. (Jack). (2016). Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems*, 33(3), 904–933. Retrieved from https://doi.org/10.1080/07421222.2015.1138375

Cleeren, K., Dekimpe, M. G., & Heerde, H. J. Van. (2017). Marketing research on product-harm crises : a review , managerial implications , and an agenda for future research. *Academy of Marketing Science*, 45, 593–615. Retrieved from https://doi.org/10.1007/s11747-017-0558-1

DeWitt, T., Nguyen, D. T., & Marshall, R. (2008). Exploring customer loyalty following service recovery: The mediating effects of trust and emotions. *Journal of Service Research*, 10(3), 269–281. Retrieved from https://doi.org/10.1177/1094670507310767

Dick, A. S., & Basu, K. (1994). Customer loyalty: Toward an integrated conceptual framework.

Journal of the Academy of Marketing Science, 22(2), 99–113.

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal*, 5(6), 215–217. Retrieved from https://doi.org/10.15406/bbij.2017.05.00149

Farah, M. F. (2017). Application of the theory of planned behavior to customer switching intentions in the context of bank consolidations. *International Journal of Bank Marketing*, 35(1), 147–172. Retrieved from https://doi.org/10.1108/IJBM-01-2016-0003

Fraser, A. (2017). The real source of SA's massive data breach. Retrieved from https://www.moneyweb.co.za/news/tech/revealed-the-real-source-of-sas-massive-data-breach/

Fuller, C., Fuller, C. M., Simmering, M. J., Atinc, G., Atinc, Y., & Babin, B. J. (2016). Common methods variance detection in business research. *Journal of Business Research*, 69(8), 3192–3198. Retrieved from https://doi.org/10.1016/j.jbusres.2015.12.008

Goddard, M. (2017). Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–706. Retrieved from https://doi.org/10.2501/IJMR-2017-050

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). USER COMPENSATION AS A DATA BREACH RECOVERY ACTION: AN INVESTIGATION OF THE SONY PLAYSTATION NETWORK BREACH. *MIS Quarterly*, 41(3), 703–727.

Guarte, J. M., & Barrios, E. B. (2006). Computation Estimation Under Purposive Sampling. *Communications in Statistics - Simulation and Computation*, 35(2), 277–284. Retrieved from https://doi.org/10.1080/03610910600591610

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2007). Examining Your Data. In *Multivariate Data Analysis* (Seventh, pp. 89–151). Harlow, United Kingdom: Pearson Education Limited. Retrieved from https://doi.org/10.4324/9781351269360

Huang, W. H. (2008). The impact of other-customer failure on service satisfaction. *International Journal of Service Industry Management*, 19(4), 521–536. Retrieved from https://doi.org/10.1108/09564230810891941

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, 82(2), 85–105. Retrieved from https://doi.org/10.1509/jm.16.0124

Jung, J., Han, H., & Oh, M. (2017). Travelers' switching behavior in the airline industry from the perspective of the push-pull-mooring framework. *Journal of Tourism Management*, 59, 139–153.

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, 45(2), 208–228. Retrieved from https://doi.org/10.1007/s11747-016-0486-5

Kumar, S. (2018). Analysis in a Business Research. *Journal of General Management Research*, 5(2), 70–82.

Lăzăroiu, G., Kovacova, M., Kliestikova, J., Kubala, P., Valaskova, K., & Dengov, V. V. (2018). Data governance and automated individual decision-making in the digital privacy general data protection regulation. *Administratie Si Management Public*, 2018(31), 132–142.

Retrieved from https://doi.org/10.24818/amp/2018.31-09

Liao, H. (2007). Do it right this time: The role of employee service recovery performance in customer-perceived justice and customer loyalty after service failures. *Journal of Applied Psychology*, 92(2), 475–489. Retrieved from https://doi.org/10.1037/0021-9010.92.2.475

Malhotra, A., & Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, 14(1), 44–59. Retrieved from https://doi.org/10.1177/1094670510383409

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58. Retrieved from https://doi.org/10.1509/jm.15.0497

Martin, K. D., Kim, J. J., Palmatier, R. W., Steinhoff, L., Stewart, D. W., Walker, B. A., … Weaven, S. K. (2020). Data Privacy in Retail. *Journal of Retailing*. Retrieved from https://doi.org/https://doi.org/10.1016/j.jretai.2020.08.003

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155. Retrieved from https://doi.org/10.1007/s11747-016-0495-4

McDermott, R. (2011). Internal and External Validity. In J. Druckman, D. Green, J. Kuklinski, & A. Lupia (Eds.), *Cambridge Handbook of Experimental Political Science* (pp. 27–40). Cambridge: Cambridge University Press.

Monroe, A. E., & Lane, J. L. (2019). People Systematically Update Moral Judgments of Blame. *Journal of Personality and Social Psychology*, 116(2), 215–236. Retrieved from https://doi.org/10.1037/pspa0000137

Munyon, T. P., Jenkins, M. T., Crook, T. R., Edwards, J., & Harvey, N. P. (2019). Consequential cognition: Exploring how attribution theory sheds new light on the firm-level consequences of product recalls. *Journal of Organizational Behavior*, 40(5), 587–602. Retrieved from https://doi.org/10.1002/job.2350

Ngobo, P. V. (2017). The trajectory of customer loyalty: an empirical test of Dick and Basu's loyalty framework. *Journal of the Academy of Marketing Science*, 45(2), 229–250. Retrieved from https://doi.org/10.1007/s11747-016-0493-6

Ortiz-Ospina, Esteban Roser, M. (2019). Economic inequality by gender. Retrieved from https://ourworldindata.org/economic-inequality-by-gender

Pick, D., & Eisend, M. (2014). Buyers' perceived switching costs and switching: A meta-analytic assessment of their antecedents. *Journal of the Academy of Marketing Science*, 42(2), 186–204. Retrieved from https://doi.org/10.1007/s11747-013-0349-2

Pick, D., Thomas, J. S., Tillmanns, S., & Krafft, M. (2016). Customer win-back: the role of attributions and perceptions in customers' willingness to return. *Journal of the Academy of Marketing Science*, 44(2), 218–240. Retrieved from https://doi.org/10.1007/s11747-015-0453-6

Ping, R. A. (1993). The effects of satisfaction and structural constraints on retailer exiting, voice, loyalty, opportunism, and neglect. *Journal of Retailing*, 69(3), 320–352. Retrieved from https://doi.org/10.1016/0022-4359(93)90010-G

Porter, M. E. (2008). Strategy Strategy the Five Competitive. *Harvard Business Review*, 86(January), 78–94. Retrieved from https://doi.org/Article

Puzakova, M., Kwak, H., & Rocereto, J. F. (2013). When Humanizing Brands Goes Wrong: The Detrimental Effect of Brand Anthropomorphization Amid Product Wrongdoings. *Journal of Marketing*, 77, 81–100. Retrieved from https://doi.org/10.1509/jm.11.0510

Saunders, M., & Lewis, P. (2018). *DOING RESEARCH IN BUSINESS AND MANAGEMENT*. *Pearson* (Second). Harlow, United Kingdom: Pearson.

Sayani, H. (2015). Customer satisfaction and loyalty in the United Arab Emirates banking industry. *International Journal of Bank Marketing*, 33(3), 351–375. Retrieved from https://doi.org/10.1108/IJBM-12-2013-0148

Schoenberg, N. E., & Ravdal, H. (2000). Using vignettes in a wareness and attitudinal research. *International Journal of Social Research Methodology*, 3(1), 63–74. Retrieved from https://doi.org/10.1080/136455700294932

Sen, R., & Borle, S. (2015a). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, 32(2), 314–341. Retrieved from https://doi.org/10.1080/07421222.2015.1063315

Sen, R., & Borle, S. (2015b). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, 32(2), 314–341. Retrieved from https://doi.org/10.1080/07421222.2015.1063315

Shah, N., Irani, Z., & Sharif, A. M. (2017). Big data in an HR context: Exploring organizational change readiness, employee attitudes and behaviors. *Journal of Business Research*, 70(2017), 366–378. Retrieved from https://doi.org/10.1016/j.jbusres.2016.08.010

Shapshak, T. (2018). Liberty hack the 'biggest breach yet'. Retrieved from https://www.businesslive.co.za/fm/fm-fox/2018-06-21-liberty-hack-the-biggest-breach-yet/

Simmons, S. A., Carr, J. C., Hsu, D. K., & Shu, C. (2016). The Regulatory Fit of Serial Entrepreneurship Intentions. *Applied Psychology*, 65(3), 605–627. Retrieved from https://doi.org/10.1111/apps.12070

Skinner, E. (1996). A Guide to Constructs of Control. *Journal of Personality and Social Psychology*, 71(3), 549–570. Retrieved from https://doi.org/10.1037/0022-3514.71.3.549

Song, S., Sheinin, D. A., & Yoon, S. (2016). Effects of product failure severity and locus of causality on consumers' brand evaluation. *Social Behavior and Personality*, 44(7), 1209–1221. Retrieved from https://doi.org/10.2224/sbp.2016.44.7.1209

Stats SA. (2020). *Quarterly Labour Force Survey*. Retrieved from Pretoria: http://www.statssa.gov.za/publications/P0211/P02111stQuarter2020.pdf

Stiennon, R. (2013). Categorizing Data Breach Severity with a Breach Level Index, 1–3. Retrieved from https://breachlevelindex.com/pdf/Breach-Level-Index-WP.pdf

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *Journal of Strategic Information Systems*, 28(3), 257–274. Retrieved from https://doi.org/10.1016/j.jsis.2018.12.001

Vanvoorhis, C. R. W., & Morgan, B. L. (2007). Understanding Power and Rules of Thumb for Determining Sample Sizes. *Tutorials in Quantitative Methods for Psychology*, 3(2), 43-50. Retrieved from https://doi.org/DOI;1020982/tqmp.03.2.p043

Wan, L. C., Hui, M. K., & Wyer, R. S. (2011). The role of relationship norms in responses to service failures. *Journal of Consumer Research*, 38(2), 260–277. Retrieved from

https://doi.org/10.1086/659039

Watson, G. F., Beck, J. T., Henderson, C. M., & Palmatier, R. W. (2015). Building, measuring, and profiting from customer loyalty. *Journal of the Academy of Marketing Science*, 43(6), 790–825. Retrieved from https://doi.org/10.1007/s11747-015-0439-4

Weiner, B. (1985). An Attributional Theory of Achievement Motivation and Emotion. *Psychological Review*, 92(4), 548–573. Retrieved from https://doi.org/10.1037/0033-295X.92.4.548

Weiner, B. (2001). Reflections and Reviews Attributional Thoughts about Consumer Behavior. *Journal of Consumer Research*, 27(December 2000), 382–387.

Whelan, J., & Dawar, N. (2016). Attributions of blame following a product-harm crisis depend on consumers' attachment styles. *Marketing Letters*, 27(2), 285–294. Retrieved from https://doi.org/10.1007/s11002-014-9340-z

Wolter, J. S., Bock, D., Smith, J. S., & Cronin, J. J. (2017). Creating Ultimate Customer Loyalty Through Loyalty Conviction and Customer-Company Identification. *Journal of Retailing*, 93(4), 458–476. Retrieved from https://doi.org/10.1016/j.jretai.2017.08.004

Zhou, Z., & Ki, E. J. (2018). Does severity matter?: An investigation of crisis severity from defensive attribution theory perspective. *Public Relations Review*, 44(4), 610–618. Retrieved from https://doi.org/10.1016/j.pubrev.2018.08.008

Appendices

Appendix 1: Sample questionnaire and Consent Statement

Introduction and Consent Statement

Welcome

I am currently a student at the University of Pretoria's Gordon Institute of Business Science and completing my research project in partial fulfilment of an MBA.

I am conducting research on the impacts of data breach severity on the customer loyalty of banking customers. To that end, you are asked to read a short statement about a data breach and complete an accompanying survey about that statement. This will help us better understand the impacts of data breaches on customers and should take no more than 15 minutes of your time. Your participation is voluntary, and you can withdraw at any time without penalty. Your participation is anonymous and only aggregated data will be reported.

By completing the survey, you indicate that you voluntarily participate in this research. If you have any concerns, please contact my supervisor or me. Our details are provided below.

Researcher name: Senzosenkosi Nsibande
Email:13094590@mygibs.co.za

Phone: 0827166394

Research Supervisor: Kerry Chipp EmailChippk@gibs.co.za

*Required

Section 1: Background

1. What is your age group? *
   - 18 - 24
   - 25 - 34
   - 35 - 44
   - 45 - 54
   - 55 - 64
   - 65 +

2. Gender *
   - Female
   - Male
   - Other
   - Prefer not to say

3. What is your highest qualification? *
   - Below Grade 12
   - Grade 12 – Matric
   - College diploma
   - Bachelor's degree
   - Honours degree or equivalent
   - Master's degree
   - Doctoral degree

4. What is your annual gross salary? *
   - below R100 000
   - R100 000 - R299 000
   - R300 000 - R499 000
   - R500 000 - R699 0000
   - R700 000 - R899 000
   - R900 000 - R1.1 Million
   - More than R1.1 Million

5. Which is you primary banking institution? *
   - Absa Group Limited
   - African Bank
   - Capitec Bank
   - Discovery Bank
   - First National Bank
   - Investec Bank
   - Rand Merchant Bank
   - Nedbank
   - Post Bank

- Standard Bank
- Tyme Bank
- Other

6. Have you been a victim of a data breach?
   - Yes
   - No

7. If you answered yes to the previous question, what information was stolen?
   - Personal identifiable information (name, email, contact details, identity numbers, address)
   - Financial Access (bank account credentials, credit card details, income, investments)
   - Account Information (username/password of social media accounts, websites)
   - Behavioural information (spending behaviour, credit behaviour)
   - Other: _____

8. Select an option between 1 and 6 *
   - Option 1
   - Option 2
   - Option 3
   - Option 4
   - Option 5
   - Option 6

Section 2: Data breach scenarios 1-6

Scenario 1

Your bank has recently announced that **1000 Records** have been stolen in a data breach. The information compromised included **email address and contact Information**. In a recent media statement, the Bank advised that the data was compromised through **non-secure customer devices** and posed a **low *risk*** to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

Scenario 2

Your bank has recently announced that **10 000 Records** have been stolen in a data breach. The information compromised included **bank account and credit card data**. In a recent media statement, the Bank advised that the data was compromised through **non-secure customer devices** and posed **some risk** to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

Scenario 3

Your bank has recently announced that **over a million** Records have been stolen in a data breach. The information compromised included **bank account and credit card data**. In a recent media statement, the Bank advised that the data was compromised **through non-secure customer devices** and posed **significant risk** to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

Scenario 4

Your bank has recently announced that **1000 Records** have been stolen in a data breach. The information compromised included **email address and contact Information**. In a recent media statement, the Bank advised that the data was compromised through **a malicious employee** and posed **low risk** to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

Scenario 5

Your bank has recently announced that **10 000 Records** have been stolen in a data breach. The information compromised included **bank account and credit card data**. In a recent media statement, the Bank advised that the data was compromised through a **malicious employee** and posed **some risk** to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

Scenario 6

Your bank has recently announced that **over a million** Records have been stolen in a data breach. The information compromised included **bank account and credit card data**. In a recent media statement, the Bank advised that the data was compromised through a **malicious employee** and posed **significant risk** to customers. The company was working tirelessly with law enforcement to minimize the impact to all its customers. The bank asked customers to remain vigilant and notify them of any suspicious behaviour.

Section 3: The Cause of the breach

9. The data breach was caused by a weakness in the bank. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

10. The bank should be held responsible for the breach. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

11. Internal Bank issues contributed to the data breach. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

12. The data breach was caused by a problem inside the Bank. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

13. The Bank could have avoided the data breach. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

14. The Bank should be held accountable for the breach. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Section 4: The impact of the breach

15. I believe the causes of the breach are permanent. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

16. I believe there is a high likelihood of the breach reoccurring. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

17. The bank had the capability to stop the breach from occurring. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

18. The cause of the breach was controllable by the Bank. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

19. The bank has the resources to prevent the breach from occurring. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

20. The cause of the breach was preventable by the Bank. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Section 5: Control over personal information

21. I believe I had control over what happened to my personal information. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

22. I have a say in how my information is used by the company. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

23. It was up to me how the company uses my information. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

24. I have a say in whether my personal information is shared with others. *

	1	2	3	4	5	6	7	
Strongly disagree	◯	◯	◯	◯	◯	◯	◯	Strongly agree

Section 6: Your response to the data breach

25. Post the breach, I would likely spread negative information about the company. *

	1	2	3	4	5	6	7	
Highly unlikely	◯	◯	◯	◯	◯	◯	◯	Highly likely

26. Post the breach, I would likely bad mouth the company to my friends, relatives, or acquaintances. *

	1	2	3	4	5	6	7	
Highly unlikely	◯	◯	◯	◯	◯	◯	◯	Highly likely

27. Post the breach, I would likely tell others not to use them if asked about their products/ services. *

	1	2	3	4	5	6	7	
Highly unlikely	◯	◯	◯	◯	◯	◯	◯	Highly likely

28. Post the breach, I intend to switch to a competitor of this Bank. *

	1	2	3	4	5	6	7	
Strongly disagree	⬭	⬭	⬭	⬭	⬭	⬭	⬭	Strongly agree

29. Post the breach, I do not intend to take-up the services of this bank anymore. *

	1	2	3	4	5	6	7	
Strongly disagree	⬭	⬭	⬭	⬭	⬭	⬭	⬭	Strongly agree

30. Post the breach, I intend not to visit the bank again. *

	1	2	3	4	5	6	7	
Strongly disagree	⬭	⬭	⬭	⬭	⬭	⬭	⬭	Strongly agree

31. If the bank were to raise its prices, I would continue to be a customer of the firm. *

	1	2	3	4	5	6	7	
Strongly disagree	⬭	⬭	⬭	⬭	⬭	⬭	⬭	Strongly agree

32. I would be dedicated to doing business with this Bank. *

	1	2	3	4	5	6	7	
Highly unlikely	⬭	⬭	⬭	⬭	⬭	⬭	⬭	Highly likely

33. If a competing bank were to offer better prices or a discount on their services, I would switch. *

	1	2	3	4	5	6	7	
Highly unlikely	⬭	⬭	⬭	⬭	⬭	⬭	⬭	Highly likely

34. If another Bank offered the same product/services, but did not collect any data about your activities, how likely would you be to: *

I. Shift all my business to this new Bank.

	1	2	3	4	5	6	7	
Highly unlikely	◯	◯	◯	◯	◯	◯	◯	Highly likely

II. Try this new Bank offering

	1	2	3	4	5	6	7	
Highly unlikely	◯	◯	◯	◯	◯	◯	◯	Highly likely

III. Pay a premium to use this new Bank.

	1	2	3	4	5	6	7	
Highly unlikely	◯	◯	◯	◯	◯	◯	◯	Highly likely

35. Is there anything you would like to add about the impact of data breaches to Banking relationship?

_____

_____

_____

_____

Appendix 2: Item mean and standard deviation

Perceived Locus of causality (adapted from Zhou and Ki (2018))		Mean	Std. Deviation
LC1	The data breach was caused by a weakness in the Bank	5,17	1,836
LC2	The Bank should be held responsible for the data breach	5,73	1,637
LC3	Internal Bank issues contributed to the data breach	5,22	1,796
LC4	The data breach was caused by a problem inside the Bank	5,14	1,897
LC5	The Bank could have avoided the data breach	5,42	1,603
LC6	The Bank should be held accountable for the breach	5,74	1,690

Stability of Cause (adapted from Haung (2008))		Mean	Std. Deviation
SC1	I believe the causes of the breach are permanent	3,70	1,879
SC2	I believe there is a high likelihood of the breach reoccurring	4,50	1,758

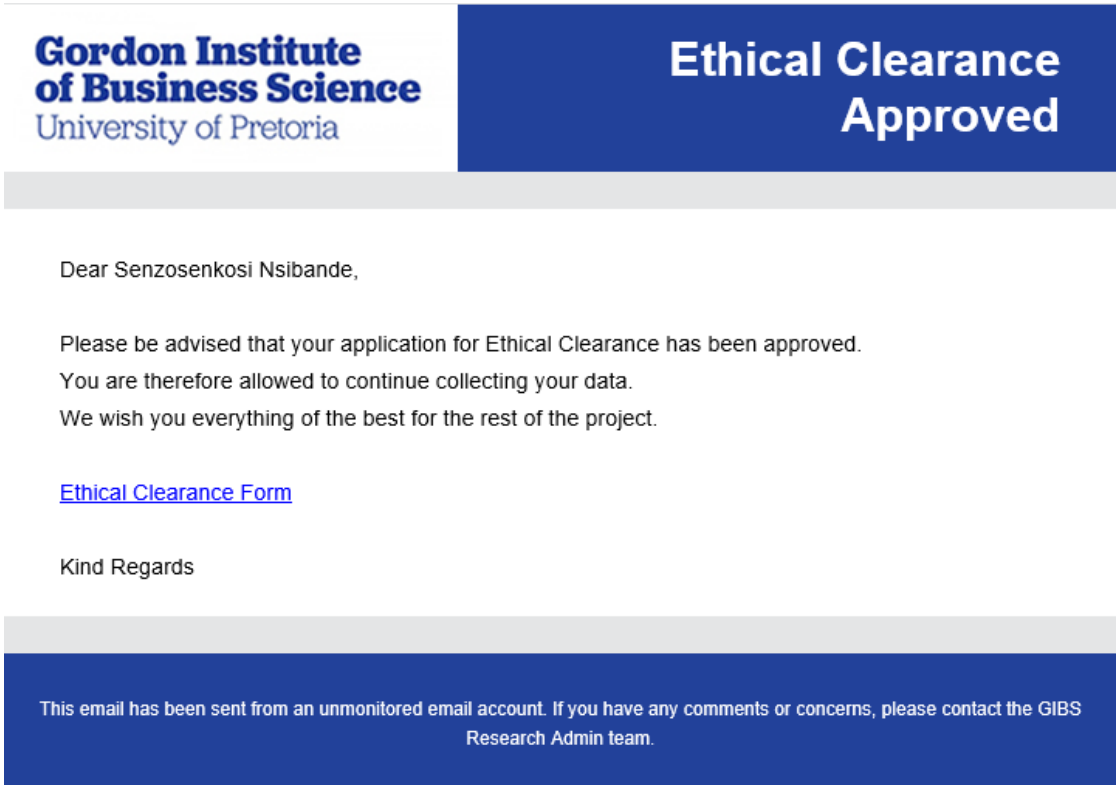
Controllability of cause (adapted from Zhou and Ki (2018) and Haung (2008))		Mean	Standard Deviation
CC1	The Bank had the capability to stop the breach from occurring	5,05	1,653
CC2	The cause of the breach was controllable by the Bank	4,66	1,808
CC3	The Bank has the resources to prevent the breach from occurring	5,55	1,569
CC4	The cause of the breach was preventable by the Bank	5,14	1,672

Customer Loyalty (adapted from Martin, Borah, and Palmatier (2017) and DeWitt, Nguyen, and Marshall (2008))			Mean	Std. Deviation
CL1	Negative Word of Mouth	Post the data breach I would likely spread negative word of mouth about the company	3,81	2,065
CL2	Negative Word of Mouth	Post the data breach I would likely bad mouth the company to my friend's relatives, or acquaintances.	3,74	2,085
CL3	Negative Word of Mouth	Post the data breach I would likely tell others not to choose them if asked about their products/ services.	3,68	2,069
CL4	Switching Behaviour	Post the data breach I intend to switch to a competitor of this Bank.	3,34	2,088
CL5	Repeat Patronage	Post the data breach I do not intend to take up the services of this Bank anymore.	3,41	2,062
CL6	Repeat Patronage	Post the data breach I intend to not visit this Bank again	3,22	2,033
CL7	Switching Behaviour	If this Bank were to raise its prices, I would continue to be a customer of the firm.	3,65	2,041
CL8	Switching Behaviour	I would be dedicated to doing business with this Bank.	3,82	1,898
CL9	Switching Behaviour	If a competing Bank were to offer better prices or a discount on their service, I would switch.	4,59	2,081

Appendix 3: Cronbach Alpha for customer loyalty

Customer Loyalty	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
CL1	.719	.844	.656
CL2	.779	.885	.643
CL3	.823	.808	.635
CL4	.812	.841	.636
CL5	.815	.873	.637
CL6	.727	.818	.655
CL7	-.436	.587	.835
CL8	-.461	.594	.831
CL9	.327	.306	.727

Appendix 4: Ethical Clearance Approval



Gordon Institute of Business Science
University of Pretoria

Ethical Clearance Approved

Dear Senzosenkosi Nsibande,

Please be advised that your application for Ethical Clearance has been approved.
You are therefore allowed to continue collecting your data.
We wish you everything of the best for the rest of the project.

Ethical Clearance Form

Kind Regards

This email has been sent from an unmonitored email account. If you have any comments or concerns, please contact the GIBS Research Admin team.