Facebook Privacy Crisis and its Impact on Organizational Trust

Adefolake T. Adedeji

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

MASTER OF ARTS (COMMUNICATION)

In the

Department of Communication Studies

Mount Saint Vincent University

June 2019

Acknowledgments

Foremost, I would like to thank God for always guiding and protecting me. I am thankful for the gift of good health and mind to complete my thesis.

I express my profound gratitude to my thesis supervisor, Dr. Alla Kushniryk for her guidance, supervision, insight and support. Her guidance helped me throughout this research, which enhanced the intellectual development that brought about the success of this work.

I would also like to thank my thesis committee, Natalie Oldfield, for her insightful comments and contributions.

My sincere appreciation goes to my parents, Dr. & Mrs. Adedeji, I appreciate your effort and support. Also, to my siblings Adeseye, Adeola, and Adedolapo, thank you and I love you.

Abstract

This study examines the impact of 2018 Facebook privacy breach crisis on users of Facebook and how it affected their trust in this organization. Situational crisis communication theory and social mediated crisis communication theory were used as theoretical frameworks. Quantitative research design was adopted, and a structured questionnaire was used to collect data. Participants of this study were 312 students, alumni and faculty members from a Canadian university. They were mostly between the ages of 19-25 (52.88%) and majority were student (92.95%). The findings of the study revealed that the participants perceived the breach of data to be an important crisis. As a result of this crisis, they did not trust Facebook and its leadership. However, they did not deem it a big enough reason to quit using social media. This research calls for the education on data privacy breaches so that people will know its implications if not taken seriously.

Table of Contents

LIST OF TABLES

1. INTRODUCTION

The internet is unarguably one of the biggest and most popular inventions of the 20th century. Through the use of this invention, a new era of user content creation and social media has been ushered in and the world has in fact become smaller. Social media are "Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content" (Kaplan & Haenlein, 2010, p. 62). Undeniably, we now exist in the era of social media and it has become an unavoidable tool of communication for individuals, organizations and even governments. Past methods of human interaction and communication have been made even simpler and faster, and newer methods have been created. Through the use of social media, people exchange photos and videos, share news, post their opinions on blogs, and partake in online discussions. Furthermore, individuals, companies, organizations and governments now interact with large audiences scattered across the globe, simply through social media. More people now prefer to communicate via social media platforms like Facebook, Twitter, and Instagram and they have served as tools to unite long-lost friends and families and also update people about interesting events in and around each other's life. Zhang and Gupta (2018) note that the significance of these platforms come from the fact that the users spend a generous amount of time to update their information and interact with other users while also surfing other member's profiles.

The Statista Portal (2018) reported that as of the second quarter of 2018, Facebook had 2.23 billion active users worldwide and it is the most popular social network worldwide. According to Pew Research Centre (2018), Facebook is the primary social media platform with two-thirds of United States adults (68%) reporting that they are Facebook users, and roughly three-quarters of those users access the social media platform on a daily basis. According to a survey conducted by

Social Media Lab (2018), 84% of online Canadian adults have a Facebook account. Just like any other organization, in which customers expect the organization to protect their privacy and be open with them, this is also expected of Facebook by its users. People sign up to Facebook with the hopes and beliefs that they can trust the platform to keep their personal information and data private which reduces the risk they face while using the platform.

Trust has become a very important issue because of the recent breaches of trust in a variety of industries and the resulting decrease in customer loyalty. According to Edelman (2018), global trust index remains on a distruster level as 20 out of the 28 countries sampled are distrusters. The United States saw a steep decline in trust across all institutions. Sixty-three percent of the U.S general population think that it's hard to recognize what is genuine news and what is fake news particularly on social media (Edelman, 2018). Trust in social media platforms have dipped by two points to 49% compared to 51% in 2017. This shows that social media platforms have the responsibility to establish and build trust among their users.

Richards, Lawrence and Burch (2011) clarified that an absence of trust harms established relationships and prompts consumers' anger and dissatisfaction, and organizations' loss of sales and competitive advantage. A major event that can damage organizational trust is crisis. Crisis is an event that no organization ever wants to experience because of its potentially damaging characteristics. It can threaten the organization's image, reputation and even destroy the organization. However, crisis is unavoidable and often comes as a surprise.

Facebook had a huge breach of data privacy crisis in March 2018 that left the data of approximately 50 million people compromised. This crisis is one of the biggest organizational crises in 2018. Users of Facebook began to delete their accounts because of the lack of trust they have in the platform, the organization and its leadership also faced a lot of scrutiny from the users,

corporate bodies, stakeholders and even the government. Facebook apologized and completely accepted the fault as theirs. Facebook placed ads that read "This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to ensure this doesn't happen again," in multiple news outlets (McKenzie, 2018,).

1.1. Statement of Purpose

It is a known fact that a public relations crisis in an organization can increase distrust customers and stakeholders have in the company. In this new era of social media, trust is more important than ever. With the emergence and adoption of new media technologies and social media, there have been a rise in cyber security threats and breach of data privacy. Millions of individuals in the world have found themselves victims of privacy breach in recent years. Currently, there is really no concise evidence about the price organizations pay for their privacy crisis. Organizations like United Airlines, H&M and Pepsi have experienced major crises in this digital age and the outrage by customers and publics were loud. However, these organizations are back to business like the crisis never happened and their customers and stakeholders are back to doing business with them.

This might not be the case for Facebook because its own crisis is a data breach. It is assumed that the public will take a breach of their data crisis as more serious than the H&M racist crisis. Using the situational crisis communication theory (Coombs, 2002) and social mediated crisis communication theory (Liu, Briones, Kuch & Jin, 2012) as frameworks, this study examines the impact of the privacy breach crisis on users of Facebook and how it affects the trust they have in this organization. The situational crisis communication theory (SCCT) explains what is expected before, during, and after a crisis and how it is best handle. The social mediated crisis

communication theory (SMCC) introduces social media as an important variable that needs to be considered while explaining crisis communication and management.

Like every crisis, it is either handled effectively or not. This study explores how organizations and their leaders can build and repair organizational trust in crisis situations like data privacy breach, best practices in crisis communication and management, and the role social media play during crises. This study aims to establish if trust is an important factor in organizational success, and, in case of Facebook's privacy breach, whether or not the trust was lost; and if a good crisis communication can improve the trust customers and stakeholders have in an organization and most especially if it can bring back the trust they have in the organization in a situation where their data privacy has been compromised. In addition, the study explores how crises especially on social media, can be managed in effective ways in order to earn customers' and stakeholders' trust back. Therefore, the following research question has been offered:

1.2. Research Question

- What are the factors that influence people's attitudes to Facebook's breach of data privacy crisis?

1.3. Defining Terms

In this study, I use some terms and I define them below

- Customer: A customer is an individual or organization that purchases, receives or consumes products, which can be in form of goods and services, and has the ability to choose between different products and suppliers (Business dictionary; Hope et al., 2017).
- Consumer: A consumer is the end user of goods and services. They are not necessarily the individual or group of people who purchase the products (Business dictionary; Hope et al., 2017).

- Stakeholder: A Stakeholder is an individual, group or organization that can influence and can be influenced by the activities, objectives, actions, and policies of an organization. A stakeholder focuses on the performance and profitability of the organization (Business dictionary).

1.4. Facebook Privacy Crisis

In March 2018, it was discovered that there had been a breach in the privacy of Facebook users and this led to a privacy breach crisis. This was not the first crisis Facebook has had in regard to the privacy of its users. Facebook has more than a decade-long track record of incidents highlighting inadequate and insufficient measures to protect data privacy, but this particular crisis affected a large number of people. This crisis was extremely huge that Facebook's CEO, Mark Zuckerberg, was invited to testify before the U.S. congress and also invited to explain to the British Parliament committee how the privacy breach happened. Facebook's privacy crisis also affected a wide range of industries like media industry and the tech industry. Customers began to request for the safety of their data which the organizations have access to. The technology sector also started receiving a lot of attention as the congress extended open invitations to the CEOs for questioning about consumer protection and data privacy. Walden Greg, a member of the Congress, wrote in the San Francisco Chronicle (May 14, 2018) stating:

> …as we in Congress keep learning more about Facebook's use of personal data, we also want consumers to have the full picture about Google's advertising model, Twitter's algorithms, and Apple's data collection practices. We want to examine how dangerous content continues to exist on YouTube, how Amazon has disrupted the retail industry, how Netflix prioritizes content across networks, and much more.

The crisis had a huge negative impact on the Facebook brand and the organization has been having a difficult time trying to restore the trust their customers and stakeholders have in them.

1.4.1. Background

On the 16th of March 2018, The Guardian, The New York Times and Channel 4 reported that Cambridge Analytica, a data mining firm, had improperly obtained access to more than 50 million Facebook user profiles. The report claimed that they have had access to this data for more than two years. However, Mark Zuckerberg, CEO Facebook, and his team did not make any comment and remark about this revelation for five days and on the fifth day Zuckerberg wrote a Facebook post and granted a CNN interview.

1.4.2. Timeline of Events

This chapter presents the timeline of events as narrated by Facebook CEO, Mark Zuckerberg, in his official press release on the 21st of March 2018.

In 2007, Facebook (FB) launched a platform with a vision that more apps should be social. In order to make this possible, FB enabled people to log into apps and share who their friends were and some information about them. Facebook's platform API also allowed developers access data and information of the users and their friends.

In 2013, a university of Cambridge researcher, Aleksandr Kogan created a personality quiz app called "thisisyourdigitallife" and about 270,000 people downloaded and gave away their information. Kogan's app started as a seemingly innocent personality test and was more comprehensive than the usual 'what is your luckiest day?' tests (New York Times, 2018). The users were asked to complete the test in exchange for money. As a result of this, Kogan's company got access to information of about 50 million people living in the United States. These data were used to create psychological profiles of the users based on their personality measures and then

advertisements were targeted to them (The Guardian, 2018). For example, someone who likes Lady Gaga, a famous musician, will probably be an extrovert, thus will see advertisements about the new night pub.

In 2014, Kogan gave out the users' information to Cambridge Analytica unbeknownst to the users. Cambridge Analytica is a data mining firm and the idea of Kogan giving out this information to the firm is that they can learn and monitor user's likes, interactions and engagement on the Facebook platform and thus understand their personality and then affectively target political advertisement to them (psychological profiling) (The Guardian, 2018). Cambridge Analytica and Kogan obtained this information in total violation of Facebook rules and did not tell anybody who had taken the personality quiz that their data would eventually be used for political adverts targeting.

In 2014, Facebook announced that they were changing the entire platform to limit the data apps could access. Apps like that of Kogan could no longer access data about a person's friend unless that friend had also authorized the app.

In December 2015, Facebook learned for the first time from journalists at The Guardian that Kogan had shared the data set he generated from his app with Cambridge Analytica. Facebook founder said Kogan's app was immediately banned from the platform and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. Zuckerberg highlights that they provided the certifications to Facebook.

On March 17, 2018, The Guardian and The New York Times published that 50 million Facebook profiles were harvested by Cambridge Analytica. This figure was later revised to up to 87 million profiles. This information was provided by Christopher Wylie, a former employee of SCL Elections and Global Science Research which created the "thisisyourdigitallife" app. Wylie

claimed that the data from the app was sold to Cambridge Analytica, which then used the data to develop "psychographic" profiles of users, and target users with pro-Trump advertising. Cambridge Analytica denied this claim.

On March 16, 2018, a day before the story was published, according to a tweet by Carole Cadwalladr, a journalist at The Guardian, Facebook threatened to sue The Guardian over the publication of the story. Campbell Brown, the head of news partnership at Facebook in an interview on March 22 said it was "not our wisest move and if it were me, I would have probably not threatened to sue The Guardian" (CNET, 2018 paragraph 2).

On March 21, 2018, five days after The Guardian and The New York Times published the story, Mark Zuckerberg released a Facebook post to address the crisis. He gave a background information on how the privacy scandal began. Facebook accepted that this was a breach of trust between them and the users of the platform who share their data and expect them to protect it. Mark Zuckerberg in his statement said, "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you……. this was a breach of trust between Kogan, Cambridge Analytica and Facebook." According to him, the most important action to prevent this kind of crisis from happening again was taken in 2016. However, he claimed some new measures would be implemented to restrict bad people from accessing user data. All apps that had access to large amount of data prior to the 2014 data reduction access would also be investigated. A full audit of the app was to be conducted and any developer that rejects this auditing would be banned.

In addition to this, Mark Zuckerberg assured that the developer's data access would be further restricted. They would not have access to user data if the user has been away for three months without using the app. Transparency would be available as the platform will make sure

users understand which apps they have allowed to access your data. They would also be able to revoke the apps permission to the data.

1.4.3. Aftermath

This event was a serious breach of trust because the original 270,000 users had only agreed that their data could be used for academic purposes, not for targeting political campaign ads. Privacy laws everywhere state you can only use data for the purposes for which you get consent at the time of collection (OECD, 2018). Also, Kogan did not have permission to collect the personal information of the additional 87 million Facebook users who did not even know their data was collected.

On March 21, after the revelation of the breach of trust, a #DeleteFacebook campaign started to trend. The movement articulates the outrage of a public that feels its needs have been secretly replaced by financial goals and it gives a voice to widespread concern over the lack of privacy in digital environments (Quartz, 2018). Facebook users began to delete their pages including Tesla CEO, Elon Musk. The Wall Street Journal (March 28, 2018) reported that some companies suspended advertising on the platform and Facebook executives have been reaching out to advertising trade bodies, marketers and advertising agencies to inform them it is working on the audit to mitigate damages.

On March 26, 2018, Facebook placed full-page ads stating: "This was a breach of trust, and I'm sorry we didn't do more at the time. We're now taking steps to ensure this doesn't happen again," in The New York Times, The Washington Post, and The Wall Street Journal, as well as The Observer, The Sunday Times, Mail on Sunday, Sunday Mirror, Sunday Express, and Sunday Telegraph in the UK (USA TODAY, 2018).

Facebook gave follow-up information in their subsequent press releases on their blog after the major crisis. They detailed the measures they are putting in place to make sure this kind of crisis does not happen again.

On April 4, 2018, Facebook announced a series of changes to data handling practices and API access capabilities. These changes include limiting the events API, which is no longer able to access the guest list or wall posts. Also, Facebook removed the ability to search for users by phone number or email address and made changes to the account recovery process to fight scraping.

On April 6, Techcrunch (2018) reported that messages from Mark Zuckerberg and other high-ranking executives' powers over controlling personal information on the platform that is not available to normal users. Subsequently, Facebook announced plans to make the "unsend" option available to all users and that Zuckerberg will also be unable to unsend messages until every user has this feature.

On April 10, 2018, Facebook announced the launch of its data abuse bug bounty program. While Facebook has an existing security bug bounty program, this data abuse bug bounty is targeted specifically to prevent malicious users from engaging in data harvesting and also reward anyone who report any misuse of data by app developers.

On April 10 and 11, 2018, Mark Zuckerberg was ordered to answer to the United States Congress in a hearing where he was questioned by senators and representatives about the company's handling of user information. Lawmakers became more interested in Facebook data breach crisis because of the revelations that Russians meddled in the 2016 election with the help of big technology companies (CNN, 2018). He was asked almost 600 questions which included whether the company should be more regulated, what the Russians did on Facebook during the

2016 election and if the platform intentionally censors conservative content. Mark Zuckerberg again apologized and admitted that the crisis was his fault.

Although Zuckerberg said that the company hasn't seen a meaningful drop off in cumulative users, a survey of 1,000 American by Techpinions (2018) released on April 12 claimed that 9% of Americans may have deleted their accounts completely due to privacy concerns that have come to light amid the crisis. 17% deleted their Facebook app from their phone and 11% deleted from other devices.

On April 19, 2018, Facebook released their updated privacy policy which spells out more clearly how it collects and uses information about its users. The updated policy helps users understand how the company turns their data into tailored advertisements, academic research and personalized recommendations.

On May 14, 2018, around 200 apps were suspended from Facebook as part of an investigation into if companies have abused APIs to harvest personal information. These apps will be banned if they are found to have misused data.

During the course of this privacy crisis, Facebook stocks dropped from $185.09 on Friday, March 16 to $172.56 on Monday, March 19. The stock prices began to drop at a downward slope with the lowest drop being on March 27 at $152.22. However, it returned back to average of 173.59 by April 27, 2018 and peaked $185.53 on May 10. This shows that the crisis only had a negative effect on the stock prices for a period of seven weeks.

Advertisers who are the backbone of Facebook began to suspend their services on the platform. Pop Boys, a United State auto parts retailer suspended all advertising on Facebook. Prior to Pop Boys, Mozzila Corp, an internet company and Germany's second largest bank Commerzbank also suspended advertising on Facebook as a result of the data breach (Financial

Post, 2018). On November 15, 2018, Rishad Tobaccowala, the chief growth officer at Publicis Groupe, one of the world's biggest advertising agency said "now we know Facebook will do whatever it takes to make money. They have absolutely no morals" (New York Times, 2018).

On July 25, 2018, Facebook revealed that 3 million users in Europe abandoned the social media platform since the breach of data event. Daily active users in Europe fell for the first time from 282 to 279 million and monthly users fell from 377 million to 376 million (The Guardian, 2018). Meanwhile in the U.S, the daily and monthly users remained the same at 185 million and 241 million, respectively (The Guardian, 2018).

On September 5, 2018, Pew Research Center (2018) released the report of the survey they conducted from May 29 to June 11, 2018. In their new survey note that 54% of Facebook users say they have adjusted their privacy settings in the last 12 months, 42% say they have taken a break from checking Facebook for a period of several weeks or more while 26% say they have deleted Facebook from their mobile phone (Pew research centre, 2018). Out of their respondents ages 18 and above, 74% of Facebook users say they have at least taken one of these three actions in the past year.

2. TRUST

2.1. Defining Trust

Trust has been a popular research topic in many disciplines over the decades. It has been explored from different perspective in disciplines like sociology, marketing, management, psychology, and even the new wave of artificial intelligence and human-computer interaction. As a result of this extensive study of trust and its interdisciplinary nature, there are multiple definitions of trust which makes it difficult to have a generic definition.

Yamagishi and Yamagishi (1994) note that trust is an elusive concept which has led to some scholars referring to the state of defining trust as a conceptual confusion (Lewis & Weigert, 1985a), a confusing pot pourri (Shapiro, 1987) and a conceptual morass (Carnevale & Wechsler, 1992). Trust has also been defined as both a noun and a verb (Barber, 1983), a belief (Lindskold, 1978), a personality trait (Rotter, 1971), a social structure (Shapiro, 1987), and a behavioural intention (Curall & Judge, 1995).

Chowdhury (2005) identify that there are two trust building foundations which are cognition-based trust and affect-based trust. Cognition-based trust is based on individual thoughts about others and the confidence, reliability and dependability in them. Cognitive-based trust is the centre of cognitive reasoning (McAllister, 1995). Cognition-based trust tends to be high when "repeated interactions allow parties to come to know, understand, and predict the routines and processes of the interaction" (Hite, 2005, p. 140). On the flip side, affect-based trust is grounded in the emotional bonds between individuals involving mutual care and concern (Chowdhury, 2005). It is more emotional than rational. According to McAllister (1995), in order for affect-based trust to exist, some form of cognition-based trust must first be present.

According to Lyons and Mehta's (1997) theory of trust there are two types of trust, such as self-interested trust (SIT) and socially-oriented trust (SOT). Self-interested trust is defined as a willingness to trust with minimal or no evidence for trust. In this situation, there is a mutual advantage to putting trust in another. Lyons and Mehta (1997) summarized SIT as forward looking with agents being trusting or trustworthy only to the extent that they expect such behaviour to yield a direct return in the future. It involves being prepared to trust someone unless proven otherwise. Socially-oriented trust (SOT) comes from self-interested trust and builds from the one-on-one relationship into a broader context. SOT is the product of either an effectual, a traditional or a value-rational behaviour orientation (Lyons & Mehta, 1997). It is generated from obligations in a social network of relationships. Lyons and Mehta (1997) note that socially-oriented trust is very fragile partly because it can be lost quickly through opportunism, and partly because people engaged in these types of contacts tend to view the possible relationship value and investment as an asset, which is subject to greater risk than that of self-interested trust. Socially-oriented trust has its root in the past. Therefore, trust can be seen as a connection between past encounters and anticipated future.

Trust develops over time. Porras (2004) notes that trust isn't static, as it is a dynamic procedure that advances as per the improvement of the relationship. According to Mayer, Davis and Schooman (1995), trust is essential in situations where uncertainty and interdependence exist. Ultimately, trust depends on a series of individual qualities of the potential partner, such as loyalty, predictability, accessibility, availability, integrity, consistency of behavior, openness, competence, benevolence, history of relationship, fairness, and the ability to keep promises (Argandona, 1999).

2.1.1. Organizational Trust

Trust is an important subject of discussion within organizations. As a result of the vagueness of the generally accepted definition of trust, the term trust is used in a group of diverse, and not always compatible ways within organisational research. It has been defined in different ways depending on the focal context. However, in the context of organizational studies, Mayer, Davis and Schoorman (1995) define trust as the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party. Paine (2003) defines organizational trust as the "organization's willingness, which is based on its culture and communication behaviours in relationships and transactions, to be appropriately vulnerable as a result of the belief that another individual, group or organization is competent, open, honest, concerned, reliable and encompass common goals, norms and values" (p. 5). Trust is important in ensuring the success of any business relationships (Halliburton & Poenaru, 2010). It even becomes more important when the business is high-risk and is characterized with uncertainty which requires customers to be vulnerable.

Singh and Sirdeshmukh (2000) note that trust acts as a safety net since it helps the customers to settle on a choice by limiting vulnerability and hazard. Dirks, Lewicki and Zaheer (2009) highlight that trust is the major element upholding the relationship between customers and the organization. Without trust on both parties, the relationship cannot survive. Trust between organizations and customers encourages quality and strong long-term relationships which subsequently make them remain loyal and committed (Aaker, Fournier & Brasel, 2004). Ndubisi (2007) in his study finds that trust is a very important factor that built loyalty and thus, there is a significant and positive relationship between trust and loyalty. For example, in the service industry,

the inability to test the service before actual consumption makes trust a valuable decision factor for customers. Therefore, engaging customers in a long-lasting and trust-based journey becomes the new goal for customer-centered organizations.

Paliszkiewicz (2010) clarifies trust as the conviction that a party won't act in a way that is hurtful to the trusting firm, the party will act so that is valuable to the trusting firm, the party will act in a dependable way and will carry on or react in a commonly acceptable way. Oldfield (2017) argues that when organizations do not develop a culture of trust with internal and external stakeholders including customers, they may experience harsh consequences if it disappears.

Existing literature on organizational studies trust mostly focus on trust between organizations and their employees (e.g.: Aryee, Budhwar & Chen, 2002; Dirks, 2000; Dirks & Ferrin, 2002) and there is a limited research on trust between organizations and their customers. Bozic (2017) explains that employees and consumer differ in their vulnerabilities, interests, power levels and expectations, and have varying levels of access, exposure and insight into an organisation's conduct. Their expectations are different, they also have conflicting interests and different proximities to the organization (Gillespie, Hurley, Dietz & Bachman, 2012).

Gounaris (2005) states that it takes time to build trust. Customers trust in an organization do not just happen overnight or in the first week of business. Trust happens from the build-up of satisfactory past experience which involves gradual deepening of relationship and mutual adjustment to the needs of the other party (Gounaris, 2005). According to Elliott and Yannopoulou (2007), customer's experience either through direct and lived experience or indirect experience of others which is usually done by word of mouth or by the organization's reputation can help organizations gain customer trust. Therefore, trust is a continuous process, reinforced by positive assessments of previous experiences and shared between customers.

Halliburton and Poenaru (2010) state that trust is created through both rational and emotional bonds. Rational trust refers to the "customer's willingness to rely on a service provider's competence and reliability" while emotional trust is a confidence that arises from the customer's "feelings generated by the level of care and concern the partner demonstrates" (Halliburton & Poenaru, 2010, p. 5). They added that there is therefore a synergy between the customer's rational and emotional engagements with an organization. A rational process involves the customer assessing the organization's intention and ability to keep promises by identifying guarantees in terms of competencies, reliability in the delivery of goods and services, and predictability of behaviors. An emotional process is when the customer evaluates the company according to the qualities and characteristics that show concern and care, as well as the willingness to compromise and act beyond a profit motive (Halliburton & Poenaru, 2010).

According to Mayer, Davis and Schooorman (1995), the factors of trustworthiness are benevolence, ability and integrity. These factors contribute a unique perspective from which to consider the trustee.

1. Ability: This is the group of skills, competencies and character that enables a party to have influence in a specific domain. Ability as a factor of trust is domain specific because the trustee may have high competence in an area and have no competence in other areas (Mayer, Davis & Schoorman, 1995).
2. Benevolence: This is the extent to which a trustee is believed to want to do good to the trustor without putting into consideration a selfish profit motive. It is the perception by customers that the object of trust demonstrates goodwill towards the customer (Mayer, Davis & Schoorman, 1995).

3. Integrity: This is the perception that the trustee follows the principles that the trustor finds acceptable. It is the belief that the organization is honest and treats stakeholders with respect (Mayer, Davis & Schoorman, 1995).

Prison and Malhotra (2011) measured stakeholder trust in an organization through four dimensions: benevolence, integrity, identification and transparency. Pirson and Malhotar (2011) explain that identification is an important factor as shared values and commitment are at the core. Identification also signifies understanding and internalization of stakeholder interest by the organization. Pirson and Malhotar (2011) concludes that transparency is a distinct dimension of trustworthiness. They refer to it as the willingness to share trust-relevant information with vulnerable stakeholders.

Communication is a very important tool that organizations must employ in building trust with customers and stakeholders. Yang and Kang (2015) note that Organization-Public Dialogic Communication (OPDC) is needed to engage in dialogue with customers. They define OPDC as "the orientation of mutuality and the climate of openness that an organization and its publics hold in communication to bring about mutually beneficial relationships" (p. 176). Yang and Kang (2015) explain that mutuality and openness must be respected in OPDC. Both organizations and customers must be willing to accommodate and tolerate the other parties' opinion while working towards finding a common ground. They must be willing to have honest and open dialogues towards the actualization of their goals (Yang & Kang, 2015).

For an organization to build customer and external stakeholder trust, there are some behaviours and attributes that good leadership of an organization should possess. Oldfield (2017) developed the Eight Principles of Building, Protecting and Strengthening Trust that when leaders and employees apply, they build, strengthen, and protect trust with customers and external

stakeholders. She highlights that trust is a tangible component of all relationships, thus, it can be measured and consequently managed. The eight principles are:

1. Listen carefully with empathy and compassion, question and involve the customer or stakeholder in dialogue that affect them: It is important for organizations to "listen and gather objective customer insights" (Oldfield, 2017 p. 91). "They need to understand their customers because building trust begins with the intention of understanding and understanding starts with listening" (Oldfield, 2017 p. 91). She qualified that listening should be done with empathy and compassion.
2. Communicate using clear, concrete, and conversational language: "Clarity inspires trust" as we only trust what we understand and believe (Oldfield, 2017 p.107). Organizations should simplify their points, avoid vague generalization and platitudes, use concrete and familiar words, make only one strong point in response to each question, support points with examples, use simple numbers and statistics, divide messages into parts, use appropriate metaphors, images and videos and support points with facts (Oldfield, 2017).
3. Be honest and transparent: Oldfield (2017) buttressed what have been discussed about transparency and she added that organizations should share as much information that they can that affects stakeholders and customers.
4. Be consistent, predictable and reliable: Customers sense of risk and vulnerability is reduced when the organization exhibits consistent, predictable and reliable behaviour (Oldfield, 2017 p. 135). According to Oldfield, 100% of the participants interviewed in her study cited reliability as the number one characteristics of trustworthy behaviour.
5. Act in the best interest of customers, stakeholders and the public: Oldfield (2017) argued that in her research, this principle is often the most difficult for organizations. "Customers

or stakeholders must believe that the organization is putting their interests first" (Oldfield, 2017 p. 153). A good way for organization to portray this is to openly communicate information in a timely manner.

6. Do the right thing; if you make a mistake fix it: As humans, mistakes are bound to happen but doing the right thing is an expression of the leader's values, integrity and ethics. "Trust can be built or broken by how an organization fixes its mistakes and the experiences customers have during an event." Oldfield (2017 p. 168) states that great and trusted leaders say they make mistakes and are not afraid to be vulnerable and thus, when they apologize it makes them sincere, genuine and authentic.
7. Deliver on your promise: "Customers want what the organization promises to deliver" therefore if organizations deliver their promises and keep commitments and integrity trust will be affirmed (Oldfield, 2017 p. 178). Organizations should track and measure their performances, follow up on their actions, improve and innovate their products and services.
8. Commit to the long term: "Organizations must continually and deliberately work to create, earn and generate trust. Leaders have the power to build and tear it down based on the cumulative actions they take, the words they speak, and how they serve" (Oldfield 2017 p. 189). She added that "committing to a long term starts with building a customer centred trust culture".

"It is impossible to apply one or two principles and not the others because they are all interconnected and all work together" (Oldfield, 2017 p. 85).

In conclusion, the lack of trust damages established relationships and leads to customers' rage and disappointment, and organisations' loss of sales and competitive advantage (Richards, Lawrence & Burch, 2011)

2.1.2. Trust in Leadership

Aryee, Budhwar and Chen (2002) argue that trust in the leadership correlates with organizational trust. Oldfield (2017) notes that trust is a "leadership imperative" (p. v). She explains that from the instances where organizations have suffered consequences of broken trust from stakeholders, it can be inferred that a customer's trust is the most important asset an organization can have.

Transparency is an important factor in building trust in leadership. Zand (1997) notes that leaders earn trust by disclosing relevant information, sharing influence and relevantly using knowledge (p. 3). Vogelgesang (2008) also reiterates that leader and follower transparency require interaction characterized by sharing relevant information, being open to giving and receiving feedback, being forthcoming regarding motives and the reasoning behind decisions, and displaying association between words and actions. These components of transparency by authentic leadership represent the value of openness in leader and follower relationship where they openly share information about each other's true thoughts and feelings (Kernis, 2003). A leader who is open and who self-discloses is expected to instill higher levels of trust in their followers (Kernis, 2003).

"Trusted leaders are not necessarily liked or loved, although some may be, but they are people whom their followers have confidence in how they use knowledge and power" (Zand, 1997 p. 3). Zand explains further that they earn trust by being fair in their dealing with others which incudes, fulfilling the spirit of their agreement, sharing rewards and hard times and not abusing power.

Zhu et al. (2013) clarifies that followers' confidence in the leader's capability is an element of cognitive based trust. They explain that cognitive trust depends on the followers' assessment of the leader which evaluates if the leader has shown integrity, competence, transparency and

reliability in the past. McAllister (1995) argued that when a baseline level of cognition-based trust is met, followers are more willing to form emotional attachment with a leader. Therefore, it can be inferred that cognition-based trust influences affect-based trust.

Apart from creating transparency, according to Covey (2009) effective leaders use 12 behaviors to build and maintain trust: talk straight, show respect, right wrongs, show loyalty, deliver results, get better, confront reality, clarify expectations, practice accountability, listen first, keep commitments, and extend trust first. A leader needs to make sure these behaviours are evenly used because if any of them is over-used or under-used, it can become a liability (Covey, 2009).

Based on the literature discussed in this chapter, I propose the following hypotheses:

H1: There is a positive relationship between perceived trust in the organization and trust in the leader of this organization.

2.1.3. Trust and Social media

Honesty, transparency and truthfulness are characteristics that are valued in the digital space. Scott (2015) notes that in such a liberal channel like social media, not disclosing sufficient information and not giving credit to people is considered to be bad and unethical. Bryson (2017) argues that it is more difficult to build trust online than it is in the physical world. She notes that organizations must "fight skepticism, a lack of control over social media platform quality, and customer reactions" (Bryson 2017, para. 2).

Information from user generated content platforms like Facebook, Twitter, and Instagram are not viewed with the same level of authenticity as the traditional media, therefore, there is a demand of higher standard of quality on social media if organizations are to become a trusted source (Bryson, 2017). Ahearne, Hughes and Schillewaert (2007) note that if an organization's

expressions on social media are handled professionally and patiently while also exercising caution against hurting the expectations of customers, their level of trust tends to increase.

Ingram et al. (2007) explain that any trust building activity that an organization showcases on social media should not just be a superficial activity; rather it should aim at earning the trust of customers. Consequently, customer trust in an organization is not only dependent on fulfilling the expectations with respect to product or services, but also in the commitment of top management of the organization to giving them the best experience (Beinhocker, Davis, & Mendonca, 2010).

Lai and Turban (2008) explain that in online social platforms, trust is both a micro and a macro-level experience in which there is an exchange between the macro network created by the actor who designed it and the micro-groups formed by individual network users. According to Bryson (2017), the popularity and open nature of social platforms have made users increasingly become concerned about privacy. She notes that it is important to build trust on social media platforms so that members can share their thoughts and experiences in an open and honest ways without the fear of privacy breach. Bryson (2017) concluded that lack of trust in the social media goes against the vision of connecting people as members may not feel comfortable using the networks.

2.2. PRIVACY AND TRUST

2.2.1 Breach of Privacy

The global principles of privacy are reflected in Article 12 of the United Nations Universal Declaration of Human Rights (Rooy & Bus, 2010). It states that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks” (UDHR, Article 12). According to Rooy and Bus (2010),

> Privacy has many aspects- it relates to culture, history, morality, the position of individuals in society, public and private security, legislation, economics, technology etc. In many societies it is an important concern underpinning societal values, in particular for sustaining freedom and the ability to exert democratic rights and human self-determination. The concept of privacy is subject to change over time; it is contextual and cultural. (p. 399)

Backman (2011) explained that a privacy breach occurs when "an individual's personal information is accessed, collected, used or disclosed in contravention of applicable privacy legislation or privacy policy" p.1. He notes that personal information which refers to information about an identifiable individual is the cornerstone to most privacy laws. This personal information can include; race, religion, age, education, political affiliation, sexual orientation and many more. Pierson (2009) further states that data breaches represent the most prevalent privacy risk arising from loss of control of information in either electronic or paper form by an organization, its business associates, or a malicious third party.

A breach of data privacy can expose individuals to risks such as embarrassment, loss of employment opportunity, loss of business opportunity, physical risks to safety and identity theft. Blackman (2011) highlights that financial loss and identity theft have been recognized as two of the most serious and fastest growing crimes in North America.

Coombs (2014) identified that a crisis can create three threats which are; public safety, financial loss and reputation loss. These threats are closely related as they all cause damage to either the organization or the public (customer). In the situation of a data privacy breach, the most important crisis threat is public safety, and this is because people's information is put out there in an unethical way and thus can be used to control and manipulate their decision-making process.

Organizations in turn, suffer financial loss which can lead to decline in their stock price and consequently reputation loss because the trust customers have in them is reduced or completely eliminated.

A privacy breach can either be intentional or involuntarily. Blackman (2011) said intentional breaches are often malicious in nature and consist of a deliberate desire to access, collect, use or disclose an individual's personal information with a view of causing a disturbance or perpetrating a crime. Intentional breaches can consist of theft or hacking or an abuse and manipulation of technologies that are used to protect personal information (Blackman, 2011).

Although hacking and theft cause risks to individuals whose personal information has been exposed, he states that human error or ignorance is often the most likely cause of privacy breaches (Blackman, 2011). The privacy breaches that occur as a result of human error or ignorance usually arise in cases of careless practices, mistaken disclosures, operational, technical or communication breakdowns. The damages caused by this kind of privacy error can be just as serious as those caused by intentional breaches (Blackman, 2011).

Blackman (2011) explains that irrespective of the type of breach an organization experiences, the organization is equally responsible for the privacy breach and for having contravened privacy legislation. It is therefore vital for organizations to be sensitive of their responsibilities regarding the handling of personal information and their duties under privacy laws. A key element of an organization's responsibilities includes implementing practices designed to prevent breaches from occurring and if this happens, enabling the organization to respond in a quick, efficient and effective manner (Blackman, 2011).

According to the Identity Theft Resource Center (2018) as of July 2nd 2018, the United States have experienced 668 breaches across industry categories like Finance, Healthcare,

Government, Education and the records of 22,408,258 people were affected and exposed. In a study by Ponemon Institute in 2017 on data breach, 43% of their IT practitioner respondents and 31% of their marketers and corporate communications respondents said their organization has experienced a data breach which involved loss or theft of more than 1,000 records that contained sensitive or confidential customer or business information in the past two years. Sixty-two per cent (62%) of the consumer respondents in this study noted that in the past two years, they have been notified by a company or government agency that their personal information has been lost or stolen as a result of one or more data breaches. These statistics show that data breaches have become a common occurrence.

2.2.2. Data Privacy and Customer Trust

Rooy and Bos (2010) explain that the ability to control the release of personal information is a crucial factor for establishing levels of trust in society.

In a survey conducted by Prime Waterhouse Coopers (PWC) (2017) on whether businesses can be trusted to secure their customers' personal information, only 25% of respondents believe most companies handle their sensitive personal data responsibly. Even fewer 15% think companies will use that data to improve their lives. Eighty-eight per cent (88%) of respondents agree that the extent of their willingness to share personal information is predicated on how much they trust a given company and nearly the same number (87%) of respondents say they will take their business elsewhere if they do not trust that a company is handling their data responsibly. Ninety-two per cent (92%) of the respondents say they should be able to control the information available about them on the internet and 91% agree that companies should notify them about all data breaches. Eighty-five per cent (85%) agree that cybersecurity and privacy risk are among the biggest risks facing society while 71% find companies privacy rules difficult to understand.

PWC (2017) study on customers' attitudes found that customer trust varies by industry. Banks and hospitals tie as most trusted when it comes to privacy and cybersecurity, outranking healthcare providers, non-profits, and online retailers. However, social media companies, advertising agencies and start-ups are less trusted than firms in other sectors and need to be proactive in maintaining customer trust. Only 6% of the respondents ranked social media in the top 5 of industry that they trust.

Klynveld Peat Marwick Goerdeler (KPMG) in 2018 also conducted a similar study in which customer trust and data privacy was researched. The study was conducted across eight (8) countries - France, United Kingdom, United States, Canada, Brazil, China, India and United Arab Emirate. Thirty-eight per cent (38%) of the study's respondents said they feel high levels of anxiety about unauthorized tracking of online habits by companies, governments or criminals. Forty-eight (48%) reported having high anxiety at the prospect of hacking of their financial, medical or other personal information online. More than half (51%) of the respondents also express their anxiety about being victims of identity theft with China and Brazil most concerned at 62% and 68% respectively. UK and Canada respondents showed lesser concern about identity theft at 37% and 39% respectively (KPMG, 2018).

Like the PWC (2017) study, the KPMG (2018) study also explain that customer trust varies by industry. Trust was placed highest in the healthcare and banking and lowest in the advertising. Sixty (60%) of the respondents trust the healthcare industry with their data, 59% trust the banking industry, 54% trust the technology industry, 54% trust the retail industry, 51% trust the power and utilities industry, 49% trust the automotive industry, 46% trust the telecom industry, 45% trust the insurance industry, 43% trust the media, 39% trust wealth management industry, 37% trust the government, and 26% trust the advertising industry.

The survey by KPMG also explain that respondents are aware that companies use their data and are willing to continue to share it as long as there is some form of value exchange. The study shows that more than 75% of the respondents were willing and generally happy to give away some level of personal information in exchange for better products and services, better personalization, better value and better security.

2.2.3. Earning Back Trust after Data Breach

PWC (2017) note that customers are willing to forgive, but their trust can only be regained if companies implement real changes in the wake of a breach. It is possible that actions taken will not win back every customer, however, some measure are more likely to help the customer regain trust. Some of these actions include compensation for victims, a detailed explanation of what happened, and a clear description of the privacy policies in place. Customers want businesses to be responsive, transparent, and take steps to ensure a breach does not happen again (PWC, 2017). KPMG (2018) in their review note that in the event of a breach of data, it is very important for the organization to be upfront about the breach immediately by explaining to their customers on how they intend to fix and ensure it does not happen again.

In the survey conducted, by PWC (2017), 27% of respondents want companies to compensate victims of the breach, 22% want the organization to tell customers what happened and how it is being resolved, 5% want the organization to reaffirm its privacy policy in clear message while only 3% want apologies. This shows that apologies are not just enough during a breach of data privacy and promises to present the intention the organization has for the future will increase the confidence of customers. To further investigate the influence on data privacy on customer trust, the following hypotheses have been proposed:

H2: There is a negative relationship between one's belief that the breach of data privacy is an important issue and their overall trust in Facebook.

H3: There is a negative relationship between one's belief that the breach of data privacy is an important issue and their trust in Mark Zuckerberg.

H4: Those who are less concerned with their social media privacy have more trust in Facebook.

3. ORGANIZATIONAL CRISIS

Seeger, Sellnow and Ulmer (1998) define organizational crisis as a "specific, unexpected and non-routine event or series of events that create high levels of uncertainty and threaten, or are perceived to threaten, an organization's high priority goals" (p. 8). Pearson and Claire (1998) explain that organizational crisis is characterized by ambiguity of cause, effect and means of resolution including the belief swift decisions must be made. They (Seeger et al. 1998) note that an organizational crisis affects two sets of people and the first set are the core organization that include managers, stakeholders and employees. The second sets of people are the customers, suppliers, members of the community and even competitors. Coombs (2006a) even suggests that a crisis in one organization has the ability to threaten the entire industry.

In the situation where the crisis is handled unprofessionally, it can set off a chain reaction of other crises (Pearson & Mitroff 1993). Johansen and Frandsen (2007) offer a term for this kind chain reaction crisis and it is called a double-crisis or a communications-crisis. They defined it as "a crisis where the original crisis is superposed by a communications-crisis, as the organization fails in managing the communication processes that should have contributed to the handling of the original crisis" (Johansen & Fransen, 2007, p.79).

Although a crisis is unpredictable, it is usually not unexpected. Fargeli and Johansen (2003) strongly believe that every crisis is foreseeable except in many cases of natural disasters. According to them, the difficult part is foreseeing when the crisis will occur. As a result of this, it is necessary for an organization to have crisis communication practitioners and strategies in preparation for any crisis. Dilenschneider (2000) explains that what all crises have in common is that if an organization prepares itself for a crisis, it has a better chance of getting some level of control over the crisis.

3.1 Crisis Management

The practice of dealing with crisis is called crisis management. Fearn-Banks (2001) defined crisis management as a strategic planning to prevent and respond during a crisis or negative occurrence. She notes that it is a process that removes some of the risk and uncertainty and allows the organization to be in greater control of its destiny.

Time is an important factor in crisis management. Pearson (2002) notes that the objective of organizational crisis management is to make timely decisions based on best facts and clear thinking. However, Fearn-Banks (1996) explains that in a crisis, emotions are on the edge, brains are not fully functioning, and events are occurring so rapidly that drafting a plan during crisis is unthinkable. This is why it is necessary for an organization to have a pre-made crisis management plan. A lot of organizations believe that the chances of crisis happening to them is slim and thus they wait for a crisis to occur before developing a crisis management plan. The reality is that as the business ecosystem becomes more technologically complex, organizations will begin to face a variety of threats stemming from many different internal and external sources frequently.

Mitroff and Anagnos (2001) explain that by having the right plans and means in place before a crisis occurs, the damage can be minimized and the time to recover from it can be shortened greatly. According to Regester and Larkin (2005), successfully managing a crisis situation involves recognizing that you have one, taking the appropriate actions to provide solution to the situation, letting people see that you are taking them and letting them hear you say the right things.

Crisis management can be divided into three stages. Coombs (2007c) explained that a staged approach means the divide of the crisis management function into discrete segments

executed in a specific order. Several staged approaches have been developed by crisis management experts.

Coombs (2007c), developed one comprehensive framework which is a systematic approach that blends the diverse crisis management understandings. He divides the crisis management process into the three macro stages, they are: pre-crisis, crisis, and post-crisis, and they each contain separate substages and set of actions that should be covered during that stage.

3.1.1. Coombs' Crisis Management Stages

- Pre-crisis stage: This stage involves the actions taken before the crisis occurs and it has three substages which are: signal detection, prevention and crisis preparation. Coombs (2007c) explains that crisis experts must develop a system for detecting potential crisis and once this crisis signal is detected, actions must be taken to prevent them from happening. If the crisis still occurs, they must be prepared to manage and respond to it.
- Crisis stage: This stage is activated at the beginning of the crisis and ends when the crisis is considered to be contained and resolved. It has two substages which are: crisis recognition and crisis containment. Crisis recognition is an understanding of how events are labelled and accepted as crises and the means for collecting crisis related information. Crisis containment on the other hand focuses on the organization's crisis response. Coombs (2007c) highlights that communication with stakeholders through words and action is an important part of this stage.
- Post-crisis stage: This stage highlights the key activities that must take place after the crisis and this is because crisis management does not end when the crisis ends. It has three substages which includes; evaluating crisis management, learning from the crisis and other

post crisis actions such as follow up communication with stakeholders and continued monitoring of issues related to the crisis to make sure the crisis does not occur again.

Another staged approach was developed by Mitroff (1994). His crisis management model consists of five stages:

- Signal detection: Mitroff (1994) believes that virtually all crisis leaves a trace of "early warning". In this stage, if the organization management can detect and act upon a crisis signal, crisis can be prevented before it occurs.
- Probing and prevention: This stage often takes place simultaneously with the signal detection stage. Crisis managers main objective here is to do everything within their power to prevent crisis from happening and to manage those that still happened despite their effort.
- Damage containment: In this stage, effects of the crisis is contained from spreading further and curtailed from infecting other unaffected parts of the organization.
- Recovery: It is in this stage that the organization tries to recover normal business operations so that key customers and stakeholders will not be lost.
- Learning: In this stage, the organization reflects on what was handled well and what was not during the handling of the crisis and how any other crisis can be handled better in the future.

These two approaches by Coombs and Mitroff are similar. Mitroff's model explains and gives suggestion on how to handle all stages of crisis as mentioned by Coombs while Coombs' model focuses on further breaking down the stages of crisis into substages. Johansen and Frandsen (2007) explains that the several substages in Coombs' model show that the field of crisis management have more nuances than ever and is continuously developing with an increased

interest in the pre-crisis and post-crisis stage as well as the crisis event phase. These models show that crisis management should be integrated in the organization's operation even if there is no crisis in view. A proper crisis management plan helps the organization to be proactive so that they are able to prepare for and possibly prevent the crisis.

3.2. Crisis Communication

Although crisis communication and crisis management are closely related and used interchangeably, they have distinct functions. Fearn-Banks (2002) defines crisis communication as "the dialogue between the organization and its publics prior to, during, and after the negative occurrence" (p. 2). As opposed to crisis management which just involves planning, crisis communication focuses on relaying information to people in case of crisis. Benoit (2004) states that planning cannot prevent every crisis, and, in some situations, organisations must directly respond to crisis. The communication following a crisis plays an important role in the success of eliminating the crisis and even improving the reputation of the organization (Ulmer, 2001).

According to Coombs (2005), crisis communication is the lifeblood of crisis management effort and it plays an important role in all the crisis management stages. Crisis communication response can either be verbal or non-verbal and it is important to understand the origin of the crisis before the development of an appropriate response. Spillan (2000), notes that some crisis may present opportunities for the business to change directions and achieve new goals while other crises may present very ugly and difficult circumstances that require quick responses.

Coombs (2006b) divides crisis response research into two categories: form and content. These two categories adopt different emphasis and are used depending on the type of crisis and stakeholders involved in the crisis. Form is how the response should be presented, and content is what is said.

According to Coombs (2006b), the form of a crisis response represents the most basic line of research concerning crisis response. Form is usually listings of what to do and what not to do and it recommends that crisis communication be consistent, open and quick. It is a general believe among crisis communicators that crisis response has to be timely. Regester and Larkin (2005) highlight that it is crucial for organizations experiencing crisis to tell their story, to tell it all and to tell it fast.

The content of a crisis response research is a more recent development in crisis management and it has proven to be more thorough than the form research (Coombs, 2006b). He notes that what is actually said during a crisis response has serious effects on the success of the crisis management effort. Therefore, clear communication is vital. Sturges (1994) explains three sequential categories of crisis communication content. They are:

- Instructing information: this information tells people affected by the crisis how they should physically react to it. This information comes first always as it shows that people are first priority.
- Adjusting information: this information helps people psychologically cope with the magnitude of the crisis situation. This information helps stakeholders cope with stress created by the uncertainty and potential harm of a crisis.
- Internalizing information: this information will be used by people to formulate an image about the organization. This information is focused on reputation management.

In every crisis situation, the primary concern has to be public safety. Coombs (2014) notes that a failure to address public safety intensifies the damage of the crisis.

3.3. Situational Crisis Communication Theory

Coombs (2002) developed the situational crisis communication theory. The theory was initially presented in an article by Coombs in 1995 although it was referred to as the symbolic approach to crisis management and communication at that time. It was in Coombs and Holladay (2002) that the theory was first called situational crisis communication theory (SCCT). SCCT has been developed and refined further from 1995 when the idea first started to 2007. It has been advanced into a more coherent and complete theory.

Coombs (2007d) notes that the situational crisis communication theory is inspired by the attribution theory. He explains that attribution theory provides the rationale and framework for the relationship between many of the variables used in SCCT. It is useful for conceptualizing crisis management and serves as the basis for explaining the relationship between crisis response strategies and crisis situations (Coombs, 1995).

3.3.1 Crisis Types

This is the first step in evaluating a crisis situation. Situational crisis communication theory posits that different type of crisis generate specific levels of crisis responsibilities. Coombs (2007d) explains that by identifying the crisis type, the crisis manager can anticipate how much responsibility stakeholders will attribute to the organization at the onset of the crisis and this therefore establishes the initial crisis responsibility level.

Coombs (2007) divides the crisis types into three clusters, such as

1. Victim cluster: The victim cluster includes crisis types in which the organization is considered a victim of the crisis alongside the stakeholders. The types of crisis under this cluster include; rumour, natural disaster, product tampering and workplace violence. For example, an earthquake or false and damaging information about an organization being

circulated makes the organization a victim of crisis. These types of crises produce minimal attribution of crisis responsibility which therefore presents a mild reputational threat to the organization (Coombs and Holladay, 2002; Coombs, 2007d).

2. Accidental cluster: The accidental cluster includes crisis types in which all of the crisis represents unintentional actions by the organization. It was not the intent of the organization to create the crisis. The types of crises under this cluster can include; technical error accident, challenges, and technical error product harm. A crisis resulting from equipment failure that causes an accident or causes a product to be recalled falls under this cluster. These types of crises produce moderate attribution of crisis responsibility which creates a moderate reputational threat (Coombs and Holladay, 2002; Coombs, 2007d).
3. Preventable cluster: The preventable cluster includes crisis types which involves the organization knowingly placing stakeholders at risk, taking inappropriate actions and/or human error that could have been avoided. The types of crises under this cluster can include; Human error accident, human error product harm, organizational misdeed either with injuries or without injuries and organizational management misconduct. Examples of this is when customers are deceived, or the laws and regulations are violated by the management. These crises types produce strong attributions of crisis responsibility, and therefore creates a severe reputational threat to an organization (Coombs and Holladay, 2002; Coombs, 2007d).

In a study by Coombs and Holladay (2005), the results showed that organizational preventable crisis produced the strongest feelings of anger. Crisis from the victim cluster produced the strongest feelings of sympathy, while the crisis in the accident cluster tended to produce muted emotional responses (Coombs & Holladay, 2005).

3.3.2. Intensifying Factors

Coombs (1995) note that the next step in evaluating the crisis situation is reviewing the factors that might intensify the reputational threat of the crisis. Coombs creates two factors that can intensify perception of crisis responsibility and image damage for organizations in crisis. They are

- Crisis history: This signifies whether or not an organization has had a similar crisis in the past. It is also called consistency as it highlights the likelihood that the organization has faced similar situations in the past. If an organization has experienced the same crisis repeatedly or has a history of the current crisis, it can indicate that it has an uncompleted problem that needs to be addressed (Coombs, 2007d).
- Prior relationship reputation: This is focused on how well or poorly an organization has or is perceived to have treated stakeholders in the same or other context. It reveals the relationship between history and reputation and how effectively the organization has dealt with its stakeholders in similar crisis situations. An unfavourable prior relational reputation suggests an organization shows little consideration for stakeholders across various areas and not just in a crisis situation (Coombs, 2007d).

Coombs and Holladay (2001) discovered in their study that an unfavourable crisis history or relationship history lead people to perceive the organization as having more responsibility for the crisis. On the other hand, a favourable crisis history or relationship history seem to be the same with neutral relationship. This shows that there was no benefit to a favourable crisis history or relationship history over a neutral relationship, just harm from unfavourable prior reputation (Coombs & Holladay, 2001). They conclude that when an organization has had a history of crisis or a negative relational reputation, a crisis that was originally considered a mild reputational threat

moved to the moderate threat level, and a crisis considered to be a moderate reputational threat moved to the severe threat level (Coombs 2004b). Coombs and Holladay (2001) term this the Velcro effect.

3.3.3. Crisis Response Strategy

Coombs (2004a) categorized crisis response strategy into three positions: deny, diminish and rebuild. These positions reflect the amount of responsibility an organization accept for a crisis and the amount of help that it is willing to provide for the victims of the crisis. Each of these positions represent a set of strategies that share similar communicative goals (Coombs, 2004a). Crisis response strategies are used to repair the reputation, to reduce negative affect and to prevent negative behavioural intentions (Coombs & Holladay, 2007). In 2007, Coombs listed the deny, diminish and repair strategy as primary crisis response strategy and included bolstering as a secondary crisis response strategy.

The deny strategy is used to remove any connection between the organization and the crisis. The organization will not suffer any damage from the crisis if it is not involved. It has three tactics. The attack the accuser strategy is when the crisis manager confronts the person or group claiming the organization is experiencing a crisis. The denial strategy is used when the crisis manager asserts that there is no crisis and there is low crisis responsibility. The scapegoating strategy is when the crisis manager blames some person or group outside of the organization for the crisis (Coombs, 2007d).

The diminish strategy is used to argue that the crisis is not as bad as people think it is or that the organization had no control over the crisis. Crisis managers can lessen the organization's connection to the crisis and have people view the crisis less negatively (Coombs, 2007). This will reduce the harmful effect of the crisis. It has two tactics. The excuse strategy is when the crisis

manager tries to minimize organizational responsibility by denying intent to do harm and claiming inability to control the incidents that triggered the crisis. The justification strategy is when the crisis manager tries to minimize the perceived damage caused by the crisis (Coombs, 2007).

The rebuild strategy attempts to improve the organization's reputation by offering material and symbolic forms of help to the victims. Crisis managers say and do things to benefit stakeholders and thus these positive actions offset the crisis. It has two tactics. Offering compensation involves the crisis manager offering money or gifts to the victim and offering apology means that the crisis manager signifies the organization takes full responsibility for the crisis and asks stakeholders for forgiveness (Coombs, 2007d).

Bolstering strategy is a secondary crisis response strategy. It is best used as supplements to the three primary strategies. It has three tactics. The reminder tactic is used to tell stakeholders about past good works of the organization. The ingratiation tactics is when crisis managers praise stakeholders and remind them of past good works by the organization. The victimage tactic is when crisis managers remind stakeholders that the organization is also a victim of the crisis (Coombs, 2007d).

Chiciudean and David (2013) state that crisis responsibility, crisis history, and prior relational reputation determine which crisis response strategy should be used. Coombs believes that the effectiveness of communication strategies is dependent on characteristics of the crisis situation. If the crisis situation is understood, the crisis manager can choose the most appropriate response. These crisis response strategies, in turn, affect different crisis communication outcomes including organizational reputation, and negative word-of-mouth (Coombs & Holladay, 2009). SCCT is an attempt to understand, explain, and provide prescriptive actions for crisis communication (Heath & Coombs 2006).

The world has become digitalized and building a crisis communication plan without the inclusion of social media is a step towards failed crisis management. The situational crisis communication theory does not include the role of the public as a communicator during crisis events and also the effect of medium type on organizational reputation (Liu et al., 2012). It is known that social media has given power to the public, therefore they should not be excluded. Social media can take crisis to a whole new level. The effect can be devastating as online news are unpredictable, can go viral and show complexity more than the original offline event. Coombs (2004) acknowledges that social media makes the channels used to deliver crisis responses more complex, he states that it has created the need to modify crisis communication. However, he did not incorporate this complexity into SCCT. This led to the development of a new model called social mediated crisis communication model by Liu, Briones, Kuch and Jin in 2012 discussed in the next chapter. To investigate the influence of crisis management and communication on customer trust, the following hypothesis have been proposed:

H5: Those who believe that the way the crisis was handled was proper have higher level of trust in Mark Zuckerberg.

H6: There is a positive relationship between one's belief that the way Facebook handled the crisis was proper and their trust in this organization.

H7: There is a negative relationship between one's belief that the way Facebook handled the crisis was proper and their concern for privacy.

4. SOCIAL MEDIA

4.1. Social Media and Crisis Communication

Web 2.0 and social media have increasingly become part of daily life. According to a 2018 report on usage of more than 240 countries across the world, approximately 53% of the world's population are active Internet users -an increase of 7% from 2017- and 42% have an active social media account -up 13% from 2017 (we are social, 2018).

The acceptance and popularity of social media has made it essential for every organization to use social media platforms to establish relationships with their stakeholders. Social media is starting to affect all the different dimensions of an organisation. The organisations' internal communication, the employee-employer relationships, the relationship with their stakeholder audiences, conversations and relationships with customers, business model innovation, and organisational reputation, trust and legitimacy have all been affected by social media. It has opened new dimensions that organizations use to cultivate and exploit knowledge sharing.

Organizations use social media for various purposes which can include to seek information, convey information, recruit, monitor customers and competitions and many more. However, one of the most important uses of social media by organizations is for crisis communication. The effect and use of social media in managing crisis is referred to as crisis informatics. Hager (2007) established this term and defined it broadly as the interconnectedness of people, organization, information and technology during crises. Crisis informatics' central tenet is that people use personal information and communication technology to respond to disaster in creative ways to cope with uncertainty (Palen & Anderson, 2016).

4.1.1. Impact of Social Media on Organizational Crisis and Crisis Communication

With a global audience of billons of people, social media which includes several platforms like Twitter, Facebook, and many more, have become one of the fastest growing industries in the world. Due to this growth, importance and population of people who use social networking sites, it has become a very important tool in crisis communication. Social networking sites are ushering in a new era of crisis communication between organizations and their publics.

Everyone with access to the internet and a computer or smart phone has become a content creator and in today's 24/7 news cycle, and information can be spread globally almost instantaneously. As a result of the close interconnection and engagement characteristics of social media, it provides a platform to anyone with an opinion at unimaginable speed. Crises can be created on social media, and they can spread on social media. It is often the first place that you will see a report of an incident and because it is difficult to control, a mere incident or issue can be perceived and even escalated as a crisis. It is no secret that the landscape of crisis communication has changed significantly due to the prevalence of social media.

Researchers argue that social media adds an overwhelming complexity to crisis communication and the multiple channels, user-level control of messaging and real-time delivery make social media far more complex than press release and conferences (Dougherty 2015; Jin, Liu, & Austin, 2014). Murray (2007) notes that this can be both a gift and a curse for public relations practitioners but often times it can make them feel overwhelmed. It can be a gift for public relations professional because if it is handled well, the reputation of the organization is enhanced, but if it goes to the other way, the reputation of the organization is at stake (Murray 2007).

Mie, Bansal and Pang (2010) refer to social media as a doubled-edged sword that pose both opportunities and threats for organizations. Acknowledging the impact social media has on the

organization is the first step to fight the threat it poses. Social media can act as both a trigger and a facilitator of crisis (González-Herrero & Smith, 2008). They explained further that as a trigger, social media has a different potential than traditional media in that it can provoke and cause crises ignited by social media content such as disclosed sensitive information and rumour. As a facilitator, social media reports the same crises as mainstream media, but at a faster pace which changes the strength and speed of the crisis (González-Herrero & Smith, 2008). Coombs (2014b) explains that social media has not just changed traditional organizational crisis communication, but it has also introduced an entire new reputational threat, and this is what is known as social media crisis.

With social media there is no longer such a thing as a local crisis. A crisis can explode anytime and since each individual has become a potential source of information, the monopoly of information is no longer in the hands of the organizations. Social media bypasses traditional gate-keepers regardless of industry and sector and in fact there is no expertise in the broadcasting of information, thus, it is necessary for an organization's crisis communication team to be well prepared be it to handle negative comments or address trending issues (Carey, 2018). Stephen and Malone (2012) note that since social media has created a space in which people are increasingly able to publicly and anonymously express dissent, creating and exposing issues requiring a corporate response, unpreparedness can be costly to organizations.

With social media, information now has a borderless reach. This increased spread of communication has serious implications for crisis communications. In a crisis situation, social media likely escalates the speed at which the crisis is discussed and shared, which increases, exponentially, the spread and magnitude of the crisis (Jordan- Meier, 2011; Shirky, 2008). Crises have become uncontainable within communities or even country borders; they are now a global

phenomenon. Coombs (2009) notes that crises in recent years are impacting people globally, where with new developments in technology, people around the world are able to watch as a major disaster unfolds. Crisis communicators no longer have the luxury of waiting a few hours to see where the crisis will reach because social media generates its own momentum. There is pressure because stakeholders expect the organization to communicate about the crisis in a timely manner via the social media (Gruber et al., 2015; Park, Cha, Kim & Jeong, 2012). Handling a crisis is no longer a private activity where the communication team writes a press release and sends it to media houses and stakeholders. Park et al. (2012) state that, therefore, not giving people the information, they want can leave an organization in a vulnerable and exposed state where negative content and rumours will start circulating via social media.

Baron and Philbin (2009) explain that social media impacts crisis communication in two distinct ways; first, the conversation can affect people's perception of the organization during the event in terms of their involvement in the conversation and secondly, it provides new opportunities to engage stakeholders and the media. "Hence, the internet plays a double-edged role in crisis communication. On one hand, it increases the risk of information thanks to the loss of traditional journalistic controls over the information market. On the other hand, the internet extends the possibilities of getting information in a manner that has not been available up to now" (Bucher 2002, p. 5).

4.1.2. Handling Crisis on Social Media

With the potential that organizations are faced with crisis both in their day to day physical reality and on social media, it becomes very important to use social media to leverage recovery and reputation building during crisis. "Crisis communications strategies that do not reflect the new environment of social media is at best ineffective, and-at worse-disastrous" (Gonzales-Herrero &

Smith, 2008). Organizations need to use social media to interact with stakeholders during crisis. Jin, Liu and Austin (2014) argue that "organizations no longer have a choice about whether to integrate social media into crisis management; the only choice is how to do so" (p.76). Baron and Phillbin (2009) argue that among communication professionals, it has been agreed that engagement is essential in times of crisis. Organizations need to understand that social media must be used as an arena for conversation rather than merely a channel for directing messages (Baron & Philbin, 2009).

Although, it is true that social media can add complexity to crisis communication because of the rate of information reach and engagement, it does not trump good communication practice (Coombs, 2010). For example, Ward (2011) notes that social media now pressures corporations to be more transparent. Using traditional crisis communication strategies, transparency is a major component that every public relations practitioner must take into consideration when handling a crisis but with social media, it become even much more important. In addition to transparency leading to building credibility and trust which can help to prevent crisis or minimize its resulting damage, with social media, nothing is hidden (Horn et al., 2015). If an organization is not transparent in it crisis communication, there is a probability that the deceit will be found on social media because of how open the platform is (Horn et al., 2015). The interactive, fast, and interconnected attribute of social media must be taken advantage of when an organization is going through crisis (Schultz, Utz, & Goritz, 2011).

In handling crisis on social media, a lack of or poorly developed crisis communication message can even cause more harm to an organization (Horn et al., 2015). Communication and crisis communication basics must still be adhered to even while addressing crisis on social media. A good crisis communication strategy when adopted on social media must be able to rebuild and

improve organization's reputation and stakeholders' behavioural intentions (Xia, 2013) which in turn revives organizational trust. Previous scholars (Coombs, 2014; González-Herrero & Smith 2010) have come up with methods organizations can use while addressing crisis via social media. Organizations use social media to provide status update by replying to stakeholders' information providing messages, funny messages, questions, and suggestions (Freberg, 2012; Veil et al., 2011; Ott & Theunissen, 2015). Veil et al., (2011) also recommend that in incorporating social media into crisis communication, crisis communicators should communicate with honesty, candor and openness while acknowledging the crisis. They should collaborate and coordinate with credible sources and should meet the needs of the media and remain accessible. Finally, they should accept uncertainty and ambiguity (Veil et al., 2011).

Agnes (2012) notes that there are three cores to using social media to communicate an organization's message throughout a crisis and they are; the message, the channel and the frequency. The message is the most important and it needs to stay in-line with the brand's day-to-day message and core brand values. It needs to be honest, informative and sincere (Agnes, 2012). After developing a good message to address crisis on social media, it needs to be communicated on the right channels, the right way because each social media channel has a different audience with different expectations, giving the obligation to meet these expectations while communicating a consistent and strategic message. She adds that since social media happens in real time, organizations should be consistent with updating their stakeholders in a timely manner preferably by choosing an interval of time and even if there is nothing new to report, the audiences should know as this will keep them on them on the channel and also keep the speculations and rumours to a minimum.

González-Herrero and Smith (2010) argue that many of the social media tools that threaten organisations can equally be exploited to assist the organisation in successful crisis communication. Solis (2008) highlights some of the factors that can be utilised in crisis communication online as; more direct, faster and wider communication, easier to understand stakeholders and engage in dialogue with them, and to communicate directly to stakeholders without media as a gatekeeper.

4.2. Social Mediated Crisis Communication

Social mediated crisis communication (SMCC) was developed by Liu, Briones, Kuch and Jin in 2012. This model of crisis communication builds on the SCCT framework and focuses on social media, its different channels and the type of media users (Jin et al., 2014). The SMCC model explains how the source and form of crisis information affects an organization's response options as well as recommend social mediated response strategies (Austin, Liu, & Jin, 2012).

In this model, the organization is considered a source of information however, in the event of crisis, a third party outside the organization may also function as a source of information (Liu et al. 2012). With social media, the third-party influence can be highly significant and therefore it will be beneficial to cooperate with influential social media creators (Liu et al., 2012)

The model outlines how an organization interact with three key publics who consume and produce crisis information;

- Social media creators are responsible for the creation of the information that others access.
- Social media followers closely follow the influential and access the information they disseminate.
- Social media inactives do not directly get information from social media but from other sources.

It outlines how social media distributes information among these publics and also traditional media Jin et al. (2014).

Liu et al. (2012) stated five key factors that affect how organizations may communicate information in a crisis situation. They are;

- Crisis origin: this examines if the crisis is an internal or external crisis.
- Crisis type: this examines the type of crisis and it was adopted from SCCT. They are victim cluster, accidental cluster and intentional cluster (Liu et al., 2012).
- Infrastructure: this examines if the crisis should be handled on a local level or needs to be addressed centrally. If the local level is selected, it is handled by the local department involved in the crisis while with the centralized approach the company headquarters handles the crisis (Liu et al., 2012).
- Message strategy: this examines the amount of responsibility an organization accepts for the crisis and the help it is willing to give the victims. This is also drawn from Coomb's SCCT (Liu et al., 2012).
- Message form: Schultz et al. (2010) explains that the medium can sometimes be more important than the message, and therefore should be carefully considered. In this situation, the medium will be considered as the message to achieve a successful crisis communication (Schultz et al., 2010).

4.3. Conclusion

It is without doubt that the nature of crisis communication has changed due to the emergence of social media. Social media can accelerate a crisis by exaggerating it to a level previously unreachable. Through rumours, hacking, shadow or copy-cat web-sites, web security breaks, and all forms of cyber-terrorism, social media can ignite crisis for an organization. With

social media, it is better to communicate information on crisis quickly to stakeholders and assume a proactive approach that will allow them to frame the messages as well as crisis. It is better to communicate an informative instant response than a reactive one. This can win public confidence and mitigate negative reaction and publicity.

The influence of social media in crisis communication is not all bad as it can help crisis strategy and messaging be tested and revised more or less in real time rather than having to commission a custom market research survey. In addition, the relationship with stakeholders can be handled directly, bypassing traditional gatekeepers such as the mainstream media (Pownall 2016). Organizations also now have greater insight into what their various different stakeholder groups think about them and behave towards them and with the use of videos, photographs and other tools, it is now possible to communicate factually and, critically in a crisis, emotionally.

Finally, an organization's ability to adopt a strong, transparent and timely crisis communication strategy to manage crisis on social media will consequently improve its reputation and its trust and credibility. Therefore, I propose the following hypothesis:

H8: Those who have higher trust in social media have higher trust in Facebook.

H9: Those who spend more time on social media are more concerned about privacy on social media.

Age plays an important role in how issues are viewed and the effects it has on people. Putting this into considerations, I propose the hypothesis that:

H10: Younger participants are less concerned about their data privacy on social media than older participants.

It is expected that public relations and communication students will have a more in-depth perspective about privacy crisis, crisis communication and organizational trust because they have taken classes on it. Therefore, I propose the hypothesis that

H11: Participants from the public relations and communications program believe that Facebook didn't handle the crisis well compared to other students.

5. RESEARCH METHODOLOGY

Research is an investigation taken in order to discover new facts, verify existing knowledge or obtain additional information about something with a view to solving its problem or improve its beneficial attributes. McMillan and Schumacher (2010) define research as the systematic process of collecting and logically analysing data for a given purpose. According to Collis and Hussey (2003), the purpose of research is "to review and synthesise existing knowledge, to investigate some existing situation or problem, to provide solutions to problems and to explain a new phenomenon, to generate new knowledge, or a combination of any of the above" (p. 2).

This chapter aims to evaluate and discuss the selected research design, illustrate the data collection methods and sources used in this research project. It also explains the rationale for the research design chosen. The discovered gaps in the literature are investigated through the survey research method which is used to collect and analyze data to proffer solution to the problem mentioned in this study. Finally, the procedures for analysis of the results, participants of study, measurement and ethical considerations are discussed.

5.1. Research Design and Methodology

Burns and Grove (2003) define a research design as a blueprint for conducting a study with maximum control over the factors that may interfere with the validity of the findings. Sellitz, Wrightman and Cook (1976) epitome the essence of research design when they said it is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedures.

The use of research design serves as a useful guide in the structuring of investigation carried out in this research in identifying variables and their relationship with one another.

Methodology is concerned with why, what, where, when and how data are collected and analyzed. The two main research paradigms; the positivistic, commonly refer to as quantitative, and the phenomenological paradigms, commonly refer to as qualitative, are the scientific practices and ways in which research can be conducted (Collis & Hussey, 2003).

In choosing a methodology for this research project, the nature of the different research methodologies and their key benefits were considered and the most suitable was selected.

5.2. Positivistic and Phenomenological Paradigms

A positivist orientation assumes that reality exists out there and that it is observable, stable and measurable (Merriam, 2009). The positivistic qualitative approach stems from the natural sciences and sees reality as a concrete structure which assumes that social reality is independent of us and exists regardless of whether we are aware of it (Collis and Hussey, 2003). It assumes that reality is socially constructed, that is, that there is no single, observable reality. Rather, there are multiple realities or interpretations of a single event (Merriam, 2009). Qualitative research methods generate theories and use small samples to produce rich and subjective data, which allows generalisation from one setting to another (Bryman, 2008).

Quantitative research designs emphasise objectivity in measuring and describing phenomena (McMillan & Schumacher, 2010). As such, the research entails the collection of numerical data, exhibits the relationship between theory and research, and uses large samples to produce highly specific and precise data, which allow generalisation from the sample to the population (Bryman, 2008). Measurement is an essential element of quantitative research. The establishment of reliability and validity are highly important for the assessment of the research quality. Reliability refers to the consistency of a measure of a concept and validity refers to the issue of if a created indicator estimates a concept rightfully (Collis & Hussey, 2003).

For the purpose of my study I have chosen to use a quantitative research design.

5.3. Quantitative Research

This study adopted the survey research method. According to Bowale (2008), the survey method is the most commonly used among behavioural scientist. Maricia (1970) as cited in Tejumaiye (2003) defines survey as a method for collecting and analyzing social data via highly structured and often very detailed interviews or questionnaire in order to obtain information from large numbers of respondents presumed to be a representative of a specific population. It involves drawing up a set of questions on various subjects or on various aspects of a subject to which selected member of a population are requested to react.

The survey was cross-sectional and consisted of the Likert-type questions. This type of survey is known to be an effective tool in the description and explanation of relationships between and among phenomena. In this study, the relationship between data privacy breach on Facebook and the level of trust respondents still have in Facebook was explored. The convenience sampling technique was used in reflecting the size of this study.

5.4. Participants of Study

This study was conducted in the Canadian university. Three hundred and twelve (312) students, and faculty of the university participated in the survey. The participants were chosen because they offer diverse demographics and also because they fall within the age bracket of people who are most active on social media. In addition to this, it is believed that because they are in the educational environment, they would have more knowledge about data breaches and crisis.

5.5. Measurement

The primary data of this study was obtained through the use of a structured questionnaire. Respondents had 46 questions to answer in the survey (7 demographic questions and 39 Likert scale questions). The questionnaire was designed to contain simple questions drawn from related literature and carefully chosen to address the problem of the study. Study questions presented in this questionnaire include two types of measurement and they are the close ended questions and questions that are set in the seven-point Likert scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (7), with verbal labels for scale points 2 through 6, came with each item. Four Likert-type questions were reverse coded (See Appendix A for the list of questions on the survey). The essence of the closed ended questions was designed to guide respondents in order to supply only the relevant information and answers for the study. The Likert scale was chosen so as to allow respondents express how much they agree or disagree with the statements made.

The questionnaire consisted of several subscales designed to measure respondents' attitudes toward 1) their trust in Facebook (12 items), 2) trust in Facebook leadership (6 items), 3) concern for privacy (5 items), 4) the handling of crisis by Facebook (6 items), 5) concern for privacy on social media (2 items) and 6) trust in social media (4 items). The situational crisis communication theory by Coombs (2002) and social mediated crisis communication theory by Liu, Briones, Kuch and Jin (2012) formed the foundation of the questions on crisis communication and social media. Questions measuring respondents' attitude toward trust were adapted from Yang and Kang (2015) study and also created based on the Eight Principles of Building, Protecting and Strengthening Organizational Trust (Oldfield, 2017). Yang and Kang (2015) in their study on dialogic communication, trust and distrust, created a scale for measuring organization-public dialogic communication (OPDC). The scale consisted of questions on different aspects of trust

which included fairness, transparency, openness, truthfulness and accountability. Questions adapted from Yang and Kang (2015) study were modified to address the purpose of this study. Oldfield (2017) in her book "The power of trust: How top companies build, manage and protect it" created eight principles of trust that good leadership of an organization should possess so as to build customer and external stakeholders trust.

These measurement instruments were chosen because it was necessary to give some contextual meaning to the findings of the study, as well as provide some vital information.

5.6. Data Collection Procedure

The data collection method used was both the self-administered questionnaire in person and online. This procedure was chosen because it ensures that the respondents are students of the university as they are distributed on campus. The online option was chosen in order to ensure that distance students were not excluded. The survey was administered from February 17th to April 2nd, 2019. The data collected from this survey was processed and analyzed using Statistical Package for Social Scientists (SPSS).

6. DATA ANALYSIS AND RESULT

As a part of research method, data analysis is one of the phases of measuring, analyzing and testing the research questions and hypotheses, which enables us to examine the research problem.

Data analysis is conducted in two steps by doing the descriptive analysis and then inferential analysis. In descriptive analysis section of this thesis, I present frequency tables for general information of the sample (gender, age, educational status, and type of respondents). Using frequency distribution table, demographic statistics and calculating descriptive numbers such as index of umbilical (mean) and index of dispersion (variance and standard deviation) data analysis is processed in this part. For each variable of the study, descriptive statistics are reported, and to check the reliability of each sub-scale Cronbach's Alpha reported. The inferential statistics, such as Pearson correlations and analysis of variance (ANOVA) were used to test hypotheses of this study.

6.1. Scale Values

For performing quantitative analysis through the questionnaire data, values are dedicated for each point of Likert statements and these values are used for calculating indexes.

DK= Don't Know; 7=Strongly Agree; 6=Agree; 5= Somewhat Agree; 4=Neither; 3= Somewhat Disagree; 2= Disagree; 1=Strongly Disagree.

6.2. Demographic Statistics

The participants of this study were students and faculty of a Canadian University. The participants were 19 years and above and are current Facebook users or have used Facebook in the past. The data was collected both in-person and online.

A total of 312 people participated in answering the survey questions. 117 respondents participated online while 195 people completed the paper survey. Out of the 117 respondents that participated in the online survey, only one participant did not finish the survey.

Out of the 312 respondents that participated in this survey (see Table 6.2.1), 165 (52.88%) of them were between the ages of 19 and 25. 84 (26.92%) of them were in the 26-35 age range while 29 (9.29%) were 36-45 years of age. 20 (6.41%) respondents were in the 46-54 age range, and 14 (4.49%) respondents were 55 years and above.

Table 6.2.1: Age of the participants

Age	N	%
19-25 (1)	165	52.88%
26-35 (2)	84	26.92%
36-45 (3)	29	9.29%
46-54 (4)	20	6.41%
55 and above (5)	14	4.49%

Out of 312 participants of this study, 219 (70.19%) were female while 93 (29.81%) were male.

Table 6.2.2: Gender

Sex	N	%
Female (F)	219	70.19%
Male (M)	93	29.81%

290 (92.95%) of the respondents were students while 20 (6.41%) were faculty. 2 (0.64%) of the respondents were alumni of who had just graduated.

Table 6.2.3: Status

What is your status in Mount Saint Vincent University?	N	%
Student (1)	290	92.95%
Faculty (2)	20	6.41%
Alumni	2	0.64%

Out of 290 respondents who were students at MSVU, 161 (51.50%) of them were in the Public relations or communication programs while 136 (43.59%) were not.

Table 6.2.4: Program of study

If you are a student, are you in the public relations or communication programs?		
Yes (1)	161	51.60%
No (2)	136	43.59%
No answer	15	4.81%

211 (67.63%) respondents of this study spend 0 to 1 hour on Facebook daily while 85 (27.24%) spend 2 to 4 hours. 12 (3.85%) spend 5 to 7 hours and 4 (1.28%) respondents spend 8 hours and more daily.

Table 6.2.5: Time spent on Facebook

How much time do you spend on Facebook daily?		
0-1 hour (1)	211	67.63%
2-4 hours (2)	85	27.24%
5-7 hours (3)	12	3.85%
8 hours and more (4)	4	1.28%

Thirteen (13) or 4.17% of the respondents stopped using Facebook after they learnt about the privacy breach. 71 (22.76%) adjusted their privacy setting, 38 (12.18%) started using Facebook less, and 146 (46.79%) respondents stated that nothing changed. 20 (6.41%) respondents started using other social media platforms more and 24 (7.69%) respondents said they have never heard about the privacy breach.

Table 6.2.6: Action after learning about privacy breach

After you learnt about the privacy breach, what did you do?		
I stopped using Facebook (1)	13	4.17%
I adjusted my privacy setting (2)	71	22.76%
I started using Facebook less (3)	38	12.18%
Nothing Changed (4)	146	46.79%
I started using other social media platforms more (5)	20	6.41%
I have never heard about it (6)	24	7.69%

When the respondents were asked if they participated in the #deleteFacebook campaign and consequently delete Facebook, only 2 (0.64%) of them said they participated and deleted. 6 (1.92%) said they participated and did not delete. 177 (56.73%) respondents stated that they did not participate while 127 (40.71%) respondents said they never heard about the #deleteFacebook campaign.

Table 6.2.7: Participation in the #deleteFacebook campaign

Did you participate in the #deleteFacebook campaign and deleted your Facebook account?	N	%
Yes, I participated and deleted (1)	2	0.64%
Yes, I participated and did not delete (2)	6	1.92%
No, I did not participate (3)	177	56.73%
I never heard about it (4)	127	40.71%

6.3. Likert Scale Statistics

This segment highlights the questions which has the highest or lowest number of respondents who chose the ‘strongly agree’, ‘strongly disagree’ and ‘don’t’ know option. For more information see Appendix C.

‘Don’t Know’ responses:

When the participants were asked if they agreed or disagreed with the statement that they believe the information Facebook gave in regard to the privacy breach crisis was genuine and complete, 51 (16.35%) were not able to answer this question and stated that they didn’t know.

Forty-Four (44) or 14.10% respondents stated that they didn't know when they were asked whether they agreed or disagreed with the statement that Facebook has taken care of every loose end and another breach of data privacy will not happen.

When the participants were asked if they agreed or disagreed with the statement that Mark Zuckerberg is proactive in righting Facebook's wrong, 44 (14.10%) stated that they didn't know.

Sixty (60) or 19.23% respondents stated that they didn't know when they were asked about the scale in which they agreed or disagreed with the statement that Facebook intentionally sells their data. This statement had the highest number of respondents who chose the "don't know" option.

When the participants were asked of the scale in which they agreed or disagreed with the statement that Mark Zuckerberg will not intentionally lie to increase Facebook's profit, 45 (14.42%) responded that they didn't know.

'Strongly Agree' responses:

When the participants were asked about the extent in which they agreed or disagreed with the statement that Facebook acts in its users' best interest, none of the respondents strongly agreed with the statement.

More than half of the respondents 169 (54.17%) answered that they strongly agreed with the statement that breach of data privacy was an important crisis.

Seventy-Eight (78) or 25% respondents answered that they strongly agreed when they were asked about the extent in which they agreed or disagreed with the statement that breach of data privacy had become very common, so they have accepted that it would happen.

125 (40.06%) respondents answered that they strongly agreed when they were asked about the extent in which they agreed or disagreed with the statement that the way a crisis was handled had an impact on how they viewed the organization.

'Strongly Disagree' responses:

When the participants were asked about the extent in which they agreed or disagreed with the statement that Facebook responded to the privacy breach accusation five days after it was first reported, and this was an appropriate amount of time, 75 (24.04%) respondents strongly disagreed with the statement.

Sixty-Five (65) or 20.83% respondents answered that they strongly disagreed when they were asked about the extent in which they agreed or disagreed with the statement "I trust Facebook".

When the participants were asked about the extent in which they agreed or disagreed with the statement that breach of data privacy was an important crisis, none of the respondents strongly disagreed with the statement.

Seventy-Two (72) or 23.08% respondents answered that they strongly disagreed when they were asked about the extent in which they agreed or disagreed with the statement that Facebook has taken care of every loose end and another breach of data privacy would not happen.

6.4. Statements with the Highest and the Lowest Means

This segment highlights the scale statistics with relations to the statements with the highest and lowers means. See Appendix D for complete information about all statements. The participants evaluated each statement on a scale of 1 to 7 with 1 as strongly disagree, 4 as neutral and 7 as strongly agree. The top three statements with the highest means, which show that the participants mostly agreed or strongly agreed with those statements, are the following:

1. Breach of data privacy is an important crisis- this statement has a mean of 6.39;
2. The way a crisis is handled has an impact on how I view the organization- this statement has a mean of 6.03;
3. A swift response by an organization on social media during a crisis contributes to restoring the trust I have in them- this statement has a mean of 5.60.

The bottom three statements with the lowest mean, meaning that the participants mostly disagree or strongly disagree with the statements are:

1. I trust Facebook – this statement has a mean score of 2.67;
2. Facebook responded to the privacy breach accusation five days after it was first reported. This is an appropriate amount of time- this statement has a mean score of 2.47
3. Facebook has taken care of every loose end and another breach of data privacy will not happen- this statement has a mean score of 2.45

Participants have a neutral attitude to the statement Facebook messages are always easy to understand and it has a mean score of 4.09.

6.5. Descriptive Statistics for Variables

Trust was measured by questions that were adapted and modified from Yang and Kang (2015) and created based on Oldfield's (2017) model of Trust. The questions examined different aspects of trust such as fairness, transparency, openness, truthfulness and accountability. A 12 item, 7-point Likert-type summated ratings scale (*1= strongly disagree; 7= strongly agree*) was used to measure respondents' ratings of trust in Facebook. See table 1 for item statistics. The highest mean is 4.09 while the lowest mean is 2.67 presented in Table 6.5.1. Overall average mean on the measurement of trust people have in Facebook is 3.131 and this shows that the respondents

have low trust in Facebook. The scale had a Cronbach's alpha of .882, which is considered very reliable.

Table 6.5.1: Descriptive Distributions for Trust in Facebook

	N	Mean	Std. Deviation
Facebook pays attention to what the users say.	287	3.37	1.577
Facebook is timely in providing information to users.	276	3.20	1.531
Facebook shares all necessary information with its users.	284	2.99	1.462
Facebook is honest in communicating with its users.	279	2.90	1.313
Facebook is transparent in sharing the organization's intent.	281	2.89	1.377
Facebook's messages are always easy to understand.	292	4.09	1.634
Facebook fixes every mistake it makes.	276	3.04	1.419
Facebook keeps its promises to the users.	271	3.22	1.356
Facebook does not care about acting ethically. Reversed	283	3.36	1.515
When Facebook makes an important decision, it considers the impacts of the decision on the publics.	282	3.34	1.409
I trust Facebook	299	2.67	1.457
Facebook acts in its users' best interest.	288	3.06	1.284
Valid N (listwise)	250	3.131	

A six-item 7-point Likert-type summated ratings scale (1= strongly disagree; 7= strongly agree) was used to measure respondents' rating on trust in Facebook leadership. See Table 6.5.2 below for item statistics. The highest mean is 3.73 while the lowest mean is 2.98. Overall average mean on the measurement of respondents rating of trust in Facebook's Leader, Mark Zuckerburg is 3.324. This result highlights that the respondents have below average trust in Facebook leadership. The scale had a Cronbach's alpha of .901, which is considered very reliable.

Table 6.5.2: Descriptive Distributions for Trust in Facebook Leadership

	N	Mean	Std. Deviation
Mark Zuckerberg, the CEO and founder of Facebook has integrity.	279	3.40	1.431
Mark Zuckerberg is trustworthy.	278	3.18	1.379
Mark Zuckerberg will not intentionally lie to increase Facebook's profit.	267	2.98	1.462
Mark Zuckerberg accepts accountability for his actions.	271	3.66	1.528
Mark Zuckerberg is proactive in righting Facebook's wrong.	268	3.73	1.517
Mark Zuckerberg is reliable.	270	3.20	1.407
Valid N (listwise)	254	3.3235	

A five-item 7-point Likert-type was used to measure respondents' concern for Facebook privacy after the crisis. See table 6.5.3 for item statistics. The highest mean is 6.39 while the lowest mean is 4.81. Overall average mean on the measurement of respondents concern for privacy on Facebook after the crisis is 5.321. This result highlights that the respondents have high concern for privacy on Facebook. The scale had a Cronbach's alpha of .765, which is considered to be a very good reliability

Table 6.5.3: Descriptive Distributions for Concern for Privacy

	N	Mean	Std. Deviation
Facebook is not respectful of privacy laws.	282	4.98	1.470
Breach of data privacy is an important crisis.	297	6.39	.909
I have confidence in how Facebook uses my data. Reversed	295	5.10	1.350
I still trust Facebook in spite of the privacy breach. Reversed	294	4.81	1.433
Facebook intentionally sells my data.	252	5.12	1.569
Valid N (listwise)	245	5.3208	

To measure respondents' rating on the way in which Facebook handled the crisis, I used a six-item 7-point Likert-type scale. See Table 6.5.4 for details. The highest mean is 3.22 while the lowest mean is 2.45. Overall average mean on the measurement of respondents rating of on the way in which Facebook handled the crisis is 2.813. This result shows that the respondents have very low perception regarding the way Facebook's crisis was handled. The scale had a Cronbach's alpha of .854, which is considered very reliable.

Table 6.5.4: Descriptive Distributions for Facebook Handling of crisis

	N	Mean	Std. Deviation
Facebook's breach of data privacy crisis has affected the trust I have in Facebook negatively. Reversed	291	3.18	1.435
Facebook responded to the privacy breach accusation five days after it was first reported. This is an appropriate amount of time.	288	2.47	1.397
Facebook's privacy crisis could have been avoided. Reversed	270	3.00	1.392
The way Facebook handled the crisis has restored my trust in them.	273	3.22	1.389
I believe the information Facebook gave in regard to the privacy breach crisis is genuine and complete.	261	2.97	1.474
Facebook has taken care of every loose end and another breach of data privacy will not happen.	268	2.45	1.391
Valid N (listwise)	231	2.8131	

A two-item 7point Likert-type summated ratings scale (*1= strongly disagree; 7= strongly agree*) was used to measure respondents' rating on concern for privacy on social media. See Table 6.5.5 below for item statistics. The highest mean is 3.83 while the lowest mean is 3.15. Overall average mean on the measurement of respondents rating of on concern for privacy on social media is 3.497. This result shows that the respondents have below average concern for their privacy on social media. The scale had a Cronbach's alpha of .551, which is considered to have a satisfactory reliability.

Table 6.5.5: Descriptive Distributions for Concern for Privacy on Social Media

	N	Mean	Std. Deviation
I read privacy terms before signing up on social media.	300	3.15	1.658
Breach of data privacy is at the top of my concern when using social media.	301	3.83	1.619
Valid N (listwise)	296	3.4966	

To measure respondents' rating on trust in social media, a four-item 7point Likert-type scale was used. See table 6.5.6 below for item statistics. The highest mean is 5.60 while the lowest mean is 3.52. Overall average mean on the measurement of respondents rating of trust social media is 4.696. This result indicates that the respondents have an above average trust in social media. The scale had a Cronbach's alpha of .709, which is considered to be a good reliability

Table 6.5.6: Descriptive Distributions for Trust in Social Media

	N	Mean	Std. Deviation
I have no problem putting my personal information (such as location and activities) on social media.	304	4.51	1.804
I am not concerned about what my data is used for on social media as long as I am able to connect with people.	301	3.52	1.676
I trust an organization that uses social media to address its issues more than one who does not.	289	5.01	1.461
A swift response by an organization on social media during a crisis contributes to restoring the trust I have in them.	290	5.60	1.191
Valid N (listwise)	280	4.6964	

6.6. Hypothesis Testing

6.6.1. Trust in Facebook and trust in leadership

Hypothesis one (H1) asks if there was a positive relationship between one's trust in the organization (Facebook) and their trust in the leader of this organization (Mark Zuckerberg). To test this hypothesis, a Pearson product-moment correlation coefficient was computed to assess the relationship between the trust in Facebook and trust in Mark Zuckerberg, a Facebook leader. There was a strong correlation between the two variables, $r = 0.743$, $n = 244$, $p = .000$, thus the first hypothesis is supported. The results are presented in Appendix E.

6.6.2. Concern for Facebook privacy and trust in Facebook

Hypothesis two (H2) argues that there is a negative relationship between the one's belief that the breach of data privacy was an important issue and their overall trust in Facebook. A Pearson product-moment correlation coefficient was used to assess the relationship between concern for Facebook privacy and trust in Facebook. The Pearson product correlation test which was found to be significant $r = -0.692$, $n = 231$, $p = .000$, and this shows a strong negative relationship between the variables. According to this, the second hypothesis of this study is supported.

6.6.3. Concern for Facebook privacy and trust in leadership

Hypothesis three (H3) posited that there is a negative relationship between one's belief that the breach of data privacy was an important issue and their overall trust in Facebook leadership. A Pearson product-moment correlation test assessed whether the relationship between concern for Facebook privacy and trust in leadership existed. According to test results which is $r = -.615$, $n =$

233, p = .000, the correlation is significant. Therefore, the third hypothesis of this study is supported.

6.6.4. Concern for social media privacy and trust in Facebook

Hypothesis four (H4) debated that those who are less concerned with their social media privacy have more trust in Facebook. The Pearson product-moment correlation coefficient was computed to assess the relationship between concern for social media privacy and trust in Facebook. The correlation test was r = -0.077, n = 249, p = .229 and this is not significant. According to this P-value, the fourth hypothesis is not supported.

6.6.5. Handling of crisis and trust in Leadership

Hypothesis five (H5) argued that the those who believe that the way the crisis was handled was proper have higher level of trust in Mark Zuckerberg as the leader of Facebook. Pearson product-moment correlation test was used to assess the relationship between handling of the crisis and trust in Mark Zuckerberg. The Pearson product correlation coefficient value which was found to be r = -0.647, n = 222, p = .000 is significant, and this shows a moderately strong positive relationship between study participants' who believe that the way the crisis was handled was proper and their higher level of trust in Mark Zuckerberg. According to this, the fifth hypothesis of this study is supported.

6.6.6. Handling of crisis and trust in Facebook

Hypothesis six (H6) of this study claimed that there is a positive relationship between one's belief that the way Facebook handled the crisis was proper and their trust in this organization. Pearson product-moment correlation coefficient was computed to assess the relationship between handling of the crisis and trust in Facebook. The correlation test was r =.700, n = 221, p = .000

and shows a strong positive relationship between them. According to P-value, the sixth hypothesis is supported.

6.6.7. Handling of crisis and concern for privacy

Hypothesis seven (H7) posits that there is a negative relationship between one's belief that the way Facebook handled the crisis was proper and their concern for privacy. Pearson product-moment correlation coefficient was computed to assess the relationship between handling of the crisis and concern for privacy. There was a correlation between the two variables, $r = -0.244$, $n = 231$, $p = .000$. Overall, there was a moderate negative correlation and the seventh hypothesis is supported.

6.6.8. Trust in social media and trust in Facebook

Hypothesis eight (H8) of this study argued that those who have higher trust in social media have higher trust in Facebook. Pearson product-moment correlation coefficient was computed to assess the relationship between trust in social media and trust in Facebook. The value was found to be $r= 0.091$, $n= 243$, $p= .157$. P-value is not significant, and the eight hypotheses of this study is not supported.

6.7. One-Way Analysis of Variance

For comparing multiple groups, I use ANOVA test. See Appendix F and G for the results of analysis of variance respondents and then for each variables of the study. Considering the P-value which is 0.000 and less than 0.05 error level: ($P - value = 0.000 < 0.05$).

6.7.1. Time spent on social media and concern for privacy

To test Hypothesis nine (H9) which argued that those who spend more time on Facebook are more concerned about privacy on social media, A one-way Analysis of Variance (ANOVA) test was applied.

This hypothesis wanted to determine if there was a significant difference in the time spent on Facebook (0-1hour, 2-4 hours, 5-7 hours, 8 hours and more) by respondents and their concern about privacy on social media. A one-way Analysis of Variance (ANOVA) was calculated using the time spent on Facebook as the independent variable and concern about privacy on social media as the dependent variable. A significant difference was noted*: $F(3, 292)= 9.012$, $p < .05$*. In a follow-up to this question, a Turkey HSD post hoc was conducted. The Turkey HSD post hoc indicated that there was a significant difference between people who spend 5-7 hours on Facebook and their concern for privacy *($M = 4.83$, $SD= 1.78$)* and people who spend 0-1 hour on Facebook (*$M = 3.24$, $SD= 1.25$*). There was also a significant difference between people who spend 2-4 hours on Facebook and their concern for privacy (*$M = 3.88$, $SD= 1.37$*) and people who spend 0-1 hour on Facebook (*$M = 3.24$, $SD= 1.25$*).

Thus, hypothesis nine (H9) was supported. See Appendix G for more details.

6.7.2. Age and concern for privacy on social media

Hypothesis ten (10) wanted to determine if younger participants are less concerned about their data privacy on social media than older participants. It discussed if there was a significant difference in younger participants' (19-25) concern about privacy on social media and older participants' (26-35, 46-54 & 55 and above) concern. A one-way Analysis of Variance (ANOVA) was calculated using the age of respondents as the independent variable and concern about privacy on social media as the dependent variable. A significant difference was noted*: $F (4, 291) = 6.354$,*

p < .05. In a follow-up to this question, a Turkey HSD post hoc was conducted. The Turkey HSD post hoc indicated that there was a significant difference between 19-25-year-old respondents and their concern for privacy *(M = 3.21, SD= 1.30)* and respondents who are 55 years and above (*M = 4.62, SD= 1.36*). There was also a significant difference between 19-25-year-old users on Facebook and their concern for privacy *(M = 3.21, SD= 1.30)* and respondents who are 36-45 (*M = 4.00, SD= 1.46*). A significant difference was also seen between 19-25-year-old respondents on Facebook and their concern for privacy *(M = 3.21, SD= 1.30)* and respondents who are 46-54-year-old (*M = 4.13, SD= 1.38*). However, the Turkey HSD post hoc test did not find a significant difference between 19-25-year-old respondents and their concern for privacy *(M = 3.21, SD= 1.30)* and respondents who are 26-35 (*M = 3.57, SD= 1.29*).

Thus, Hypothesis ten (H10) was supported. See Appendix F for more information.

6.8. Independent Samples t-Test

Hypothesis eleven (H11) argued that those from the public relations and communications program believe that Facebook didn't handle the crisis well compared to other students.

An independent *t*-test was conducted to determine if participants from the public relations and communications program believe that Facebook didn't handle the crisis well compared to other students. The Levene's test for equality of variance was not significant *(F = .137)* so equality of variance cannot be assumed, *t(155.82) = -.800, p > .05*. Thus, this hypothesis was not supported.

Table 6.9 summarizes the results of the study and presents which hypotheses were supported or rejected in the process of data analysis.

Table 6.9: Hypotheses Result

H#	HYPOTHESIS	RESULTS
H1	There is a positive relationship between perceived trust in the organization and their trust in a leader of this organization.	Supported
H2	There is a negative relationship between one's belief that the breach of data privacy is an important issue and their overall trust in Facebook.	Supported
H3	There is a negative relationship between one's belief that the breach of data privacy is an important issue and their trust in Mark Zuckerberg.	Supported
H4	Those who are less concerned with their social media privacy have more trust in Facebook.	Rejected
H5	Those who believe that the way the crisis was handled was proper have higher level of trust in Mark Zuckerberg.	Supported
H6	There is a positive relationship between one's belief that the way Facebook handled the crisis was proper and their trust in this organization.	Supported
H7	There is a negative relationship between one's belief that the way Facebook handled the crisis was proper and their concern for privacy.	Supported

H8	Those who have higher trust in social media have higher trust in Facebook.	Rejected
H9	Those who spend more time on social media are more concerned about privacy on social media.	Supported
H10	Younger participants are less concerned about their data privacy on social media than older participants.	Supported
H11	Participants from the public relations and communications program believe that Facebook didn't handle the crisis well compared to other students.	Rejected

7. FINDINGS, CONCLUSION AND RECOMMENDATIONS

7.1. Discussion of findings

The findings of this study revealed that the students and faculty of the university believe that breach of data privacy is an important crisis. Hence, with Facebook data privacy breach crisis, it was imperative to check the trust that people still have in Facebook. The study found out that, the trust respondents have in Facebook is very low. They do not think Facebook is honest, transparent, and respectful of privacy laws. They also believe that Facebook intentionally sells their data. The respondents only think that the best thing that shows how trustworthy Facebook is, is how easy it is to understand the messages they put out. In fact, when the respondents were asked if they trusted Facebook, majority of them responded negatively.

About half of the respondents claimed that they 'somewhat agree' to knowing everything about the Facebook privacy crisis. The result of the study shows that people who know everything about the Facebook crisis have negative trust towards Facebook and its leadership. They also do not think Facebook handled the crisis well. There is however a positive relationship between how much they know about the crisis and their concern for privacy on social media and on Facebook.

Although, it is possible to trust the leadership of an organization and not trust the organization, this is not the case for Facebook. This study shows that respondents also have very low trust in Mark Zuckerberg, the leader of this organization. They most especially believe that Zuckerberg would not mind lying to them as long as it increases Facebook's profit. The findings of the study agree with Aryee, Budhwar and Chen's (2002) argument that trust in the leadership correlates with organizational trust. Also, despite the damage caused by breach of privacy and their lack of trust in Facebook and its leadership, the respondents do not think it was enough reason to

stop using the platform. In this study, they agree that trust matters but this does not reflect in their behavior. They believe that it is more important to connect with family and friends than delete Facebook.

From the findings, it is seen that even though respondents see breach of data privacy as an important crisis, only a little above average believe that breach of data privacy is a top concern when using social media. Even with the low trust they have in Facebook following the crisis, less than half of the respondents read privacy terms before signing up on social media. Half of the respondents are willing to ignore what their data is used for as long as they are able to connect with other people on social media. The attitude of the respondents can be a result of the fact that a high number of respondents believe that breach of data privacy has become very common and thus, they have accepted that it will happen. Furthermore, this explains why a high percentage of the respondents (46.79%) claimed that nothing changed after learning about the Facebook privacy breach and also refused to participate in the #deleteFacebook campaign (56.73%).

Majority of the respondents believe that the way an organization handles crisis has an impact on how they view the organization. They also agree that the swifter the organization responds during crisis on social media, the more it contributes to restoring the trust they have in the organization. Based on these factors, the respondents do not believe that Facebook handled the breach of data privacy crisis well. Facebook response to the crisis five days after it was reported did not appeal to the respondents and therefore, they do not believe that the information provided by Facebook is genuine and are not confident that the data breach will not happen again. A lot of the respondents claimed that the way Facebook handled the crisis did not restore the trust they have in the organization.

Another finding of the study revealed that respondents who spend more hours on Facebook have more concern for their privacy on social media. The respondents who spend 5 to 7 hours daily have more concern about what their data is used for than people who spend 1 hour or less daily. This is expected because the longer a person spends on a social media platform, whether for work or personal use, the higher the chances of experiencing data breach and identity theft. This, in turn, makes them more concerned about what their data is being used for. People who spend little time on social media do not really have anything to worry about and thus, do not necessarily have major concern for what their data is being used for.

The study also shows that older people (36 and above) have more concern for privacy on social media than people between the ages of 19-25 and 25-35. There is particularly a huge distinction between how important privacy is on social for respondents who are 19-25 and those who are between 46 and above. This finding is supported by a survey by Rivertz (2019) which shows that younger people's (millennials) lack of concern toward data privacy is not only peculiar to social media. In this survey, the younger generations were found to be much less concerned about protecting their data than other generations. The survey explained that 66% of Gen Xers (age 40-54) and 62% of Baby Boomers (age 55-75) thought it was important that all of their Internet-of-things devices communicated securely while only 33% of millennials thought this was important.

A high number of participants responded that they were not concerned about what their data is used for on social media as long as they are able to connect with people and likewise also have no problem with putting their personal information, like location and activities, on social media. Also, only 71 (22.76%) of respondents adjusted their privacy settings after the Facebook crisis. This portrays that respondents generally do not see social media as an important aspect of

their lives in which they need to protect. Rivertz' survey backs this finding up when its respondents were asked the extent in which they were willing to protect their data based on the types of accounts in which they would enable two-factor authentication. The two-factor authentication serves as an extra layer of security and control over their data. Ninety-one (91) percent chose bank accounts, fifty-three (53) percent chose health records, forty-nine (49) percent chose email and only Thirty-Nine (39) percent chose social media.

This study also sought to find out if there was a distinction between how students in the public relations and communications program and students in other programs responded to the survey. The findings of this survey show that there were no differences between majority of the answers provided by these two groups. However, Publics Relations and Communication students know more about the Facebook breach of data privacy than all other students.

7.2. Limitations, Suggestions for Further Research and Recommendations

A major limitation of this study is that the convenience sampling method was used, thus the results are not generalizable. The participants of the study were students and faculty from a Canadian university. Students and faculty may have more knowledge about the Facebook privacy crisis as well as more information about the ways the crisis should be handled. In the future, more research should be done about the impact of privacy crisis on organizational trust by involving participants from all ages and various backgrounds. This study focused on crisis and its impact on organizational trust using the Facebook breach of data privacy as the unit of study. The study using other organizations in different industries asides tech and social media, that have also experienced data breach could be beneficial. It will be worthwhile to see if the level of trust people have post-data-breach varies.

From the findings of the study, I recommend that education on data breach needs to be provided to people especially the younger generation. A lot of people do not understand the risks and the consequences of data breaches, identity theft especially on social media and this must be taught. Trust in Facebook is at an all-time low currently and Facebook should engage in trust building activities that will appeal to their users which will help restore trust.

7.3. Conclusion

Breach of data privacy has become very common in recent times that people have accepted it as part of the unavoidable gift that comes with technology and the internet. Data breach has not only infiltrated social media but all aspects of life. However, people are more willing to look past the breach that happens on social media than in any other industries. The reaction to the March 2018 Facebook privacy breach serves as a mirror into the world of how people respond to data breaches on social media. This can tie into the believe that social media is now an integral part of living and not even a breach of data can stop people from using and engaging with it.

However, despite that fact that privacy breach is now seen as an everyday occurrence, trust still remains an important tool for the success of an organization. Breach of data privacy crisis damages the trust customers have in an organization. The study submits that although the customer may continue to use, work with or patronize the organization after a data privacy breach, the trust is never fully restored.

Finally, the study highlights that good and effective tailored crisis communication strategies can play an important role in managing the extent of damage the organization faces during and after a crisis. In the case of Facebook, even though a large number of people agree that a swift response helps in restoring trust in the organization, they also believe that a more detailed response that comes few days late can be more important than a swift response.

REFERENCES

Aaker J.L., Fournier S., & Brasel S.A. (2004). When good brands do bad. *Journal of Consumer Research*. *31*, 1-16

Agnes, M., 2012. How to use social media to communicate your message in a crisis. Retrieved from http://www.business2community.com/social-media/how-to-use-social-media-to-communicate-your-message-in-a-crisis-0201319#!zDk7e

Ahearne, M., Hughes, D. E., & Schillewaert, N. (2007). Why sales reps should welcome information technology: Measuring the impact of CRM-based IT on sales effectiveness. *International Journal of Research in Marketing, 24*(4), 336-349. doi: 10.1016/j.ijresmar.2007.09.003

Argandona, A. (1999). Sharing out in alliances: Trust and ethics. *Journal of Business Ethics*, *2*, 217-228.

Aryee, S., Budhwar, P. S., & Chen, Z. X. (2002). Trust as a mediator of the relationship between organizational justice and work outcomes: Test of a social exchange model. *Journal of Organizational Behavior, 23*, 267–285.

Austin, L., Liu, B.F. and Jin, Y. (2012). How Audiences Seek Out Crisis Information: Exploring the Social-mediated Crisis Communication Model. *Journal of Applied Communication Research*, *40*(2), 188–207.

Barber, B. (1983). *The Logic and Limits of Trust.* New Rutgers University Press, Brunswick, NJ.

Baron, G., & Philbin, J. (2009). Social media in crisis communication: Start with a drill. *Public Relations Tactics*, *16*(4), 12.

Beinhocker, E., Davis, I. & Mendonca, L. (2010). The 10 trends you have to watch. Retrieved from https://hbr.org/2009/07/the-10-trends-you-have-to-watch

Benoit, W. L. 2004. *Image restoration discourse and crisis communication. In Responding to crisis: a rhetorical approach to crisis communication,* edited by Millar, D. P. and Heath, R. L., Mahwah, NJ, USA: Lawrence Erlbaum Associates, Inc.

Blackman, P. (2011). Privacy breaches- impact, notification and strategic plans. Privacy law bulletin. Retrieved from https://www.airdberlis.com/docs/default-source/articles/privacy-law-bulletin---jan-2011.pdf?sfvrsn=2

Bozic, B. (2017). Consumer trust repair: a critical literature review. *European Management Journal. 35*(4), 538-547.

Bryman, A., Becker, S. & Sempik, J. (2008). Quality criteria for quantitative, qualitative and mixed methods research: The view from social policy. *International Journal of Social Research Methodology, 11(4),* 261-272.

Bryson, R. (2017). The importance of trust on social media. The conference board of Canada. Retrieved from https://www.conferenceboard.ca/topics/security-safety/commentaries/hot-topics-in-security-and-safety/2017/11/27/the-importance-of-trust-on-social-media

Bughin, J., & Chui, M. (2010). The rise of the networked enterprise: Web 2.0 finds its payday. *McKinsey Quarterly*. Retrieved from http://www.mckinseyquarterly.com

Burns, N. & Grove, S.K. (2003). *Understanding nursing research*. 3rd ed. Philadelphia: Saunders Company.

Business Dictionary. Customer definition. Retrieved from http://www.businessdictionary.com/definition/customer.html

Carey, L. J. (January 16, 2018). Crisis communication and social media in health care. The Fox Group LLC. Retrieved from https://www.foxgrp.com/executive-management/crisis-communication-and-social-media/

Carnevale, D. G., & Wechsler, B (1992). Trust in the public sector: individual and organizational determinants. *Administration & Society, 23*, 471-494.

Chiciudean, I., & David, G. (2013). Considerations on using the situational crisis communication theory in the crisis communication planning activities of Romanian Armed Forces' Informat. *Journal of Defense Resources Management*, 1, 159-166.

Chowdhury, S. (2005). The role of affect and cognition-based trust in complex knowledge sharing. *Journal of Managerial Issues*, *17*(3), 310-326.

CNET (March 22, 2018). Facebook: Threat to sue journalist was not our wisest move. Retrieved from https://www.cnet.com/news/facebook-threat-to-sue-paper-for-cambridge-analytica-not-wisest-move/

CNN (March 25, 2018). Facebook's Mark Zuckerberg says Sorry in full-page newspaper ads. Retrieved from https://www.cnn.com/2018/03/25/europe/facebook-zuckerberg-cambridge-analytica-sorry-ads-newspapers-intl/index.html

CNN (March 19, 2018). Facebook is facing an existential crisis. Retrieved from https://money.cnn.com/2018/03/19/technology/business/facebook-data-privacy-crisis/index.html

Collis, J. & Hussey, R. (2003). *Business Research: A Practical Guide for Undergraduate and Postgraduate Students.* Palgrave Macmillan, Houndmills, Basingstoke, Hampshire

Coombs, W. T. (1995). Choosing the right words: The development of guidelines for the selection of the "appropriate" crisis-response strategies. *Management Communication Quarterly, 8*(4), 447–476.

Coombs, W. T. (2004a). A theoretical frame for post-crisis communication: Situational crisis communication theory. In Martinko, M. J. (Ed.), *Attribution theory in the organizational sciences: Theoretical and empirical contributions* (pp. 275-296). Greenwich, CT: Information Age Publishing.

Coombs, W. T. (2004b). Impact of past crisis on current crisis communications: Insights from situational crisis communication theory. *Journal of Business Communication*, 41(3), 265-289.

Coombs, W. T. (2005a). Crisis and crisis management. In Heath, R. L. (Ed.), *Encyclopedia of public relations* (pp. 217-221). Thousand Oaks, CA: Sage.

Coombs, W. T. (2006a). *Code red in the boardroom: Crisis management as organizational DNA.* Westport, CT: Praeger.

Coombs, W. T. (2006b). Crisis management: A communicative approach. In Botan, C. H. & Hazleton, V. (Eds.). *Public Relations Theory II*. Mahwah, NJ: Lawrence Erlbaum.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: the development and application of situational crisis communication theory. *Corporate Reputation Review, 10*(3), 163-176. http://dx.doi.org/10.1057/palgrave.crr.1550049

Coombs, W. T. (2007c). *Ongoing crisis communication: Planning, managing, and responding*. Thousand Oaks, CA: Sage.

Coombs, W. (2009). Conceptualizing crisis communication. In R. L. Heath, & H.D. O'Hair (Eds.). Handbook of crisis and risk communication. (p. 100-119). New York: Routledge.

Coombs, W. T. (2011). *Ongoing crisis communication: Planning, managing, and responding*. Thousand Oaks, CA: Sage.

Coombs, W.T. (2014b). Crisis management and communications. Institute for public relations. Retrieved from https://instituteforpr.org/crisis-management-communications/

Coombs, W. T., & Holladay, S. J. (2001). An extended examination of the crisis situation: A fusion of the relational management and symbolic approaches. *Journal of Public Relations Research*, *13*, 321-340.

Coombs, W. T. & Holladay, S.J. (2002). Helping crisis managers protect reputational assets: Initial tests of the situational crisis communication theory. *Management Communication Quarterly*, *16*(2), 165–186.

Coombs, W. T., & Holladay, S. J. (2005). Exploratory study of stakeholder emotions: Affect and crisis. In Ashkanasy, N. M., Zerbe, W. J. & Hartel, C. E. J. (Eds.), *Research on emotion in organizations: Vol. 1: The effect of affect in organizational settings* (pp. 271-288). New York: Elsevier.

Coombs, W. T., & Holladay, S. J. (2007). The negative communication dynamic: Exploring the impact of stakeholder affect on behavioural intentions. *Journal of Communication Management, 11*(4), 300-312.

Covey, S. M. R. (2009). How the best leaders build trust. Retrieved from https://www.leadershipnow.com/CoveyOnTrust.html

Currall, S. C. & Judge, T. A. (1995). Measuring trust between organizational boundary role persons. *Organizational Behavior and Human Decision Processes 64*, 151-170.

Dilenschneider, R. L. (2000). *The Corporate Communications Bible: Everything You Need to Know to Become a Public Relations Expert*. Beverly Hills: New Millennium Press.

Dirks, K. T. (2000). Trust in leadership and team performance: Evidence from NCAA Basketball. *Journal of applied psychology. 85*(6), 1004-1012.

Dirks, K. T., & Ferrin, D. L. (2002). Trust in Leadership: Meta-Analytic Findings and Implications for Research and Practice. *Journal of applied psychology. 87*(4), 611-628.

Dirks, K. T., Lewicki, R. J., & Zaheer, A. (2009). Repairing relationships within and between organizations: Building a conceptual foundation. *The Academy of Management Review. 34*(1), 68-84. http://dx.doi.org/10.5465/AMR.2009.35713285

Dougherty, J. (2015). 6 social media musts for crisis communication. Retrieved from https://www.cision.com/us/2015/06/6-social-media-musts-for-crisis-communication/

Edelman PR (2018). 2018 Edelman Trust Barometer Global Report. Retrieved from https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf

Elliot, R. & Yannopoulou, N. (2007). The nature of trust in brands: A psychosocial model. *European Journal of Marketing 41*(10), 988-998.

Facebook (April 19, 2018). Data policy. Retrieved from https://www.facebook.com/about/privacy/update/printable

Facebook Investor Relations (2018). Facebook stock data and stock chart. Retrieved from https://investor.fb.com/stock-information/default.aspx

Facebook Newsroom (April 4, 2018). An update on our plans to reduce data access on Facebook. Retrieved from https://newsroom.fb.com/news/2018/04/restricting-data-access/

Facebook Newsroom (April 10, 2018). Data abuse bounty: Facebook now rewards for report of data abuse. Retrieved from https://newsroom.fb.com/news/2018/04/data-abuse-bounty/

Facebook Newsroom (May 14, 2018). An update on our app investigation and audit. Retrieved from https://newsroom.fb.com/news/2018/05/update-on-app-audit/

Fagerli, H.P. & Johansen, B.R. (2003). *Crisis management in corporate communication: A Strategic approach to building reputation.* Oslo: Gyldendal Akademisk.

Fearn-Banks, K. (1996). *LEA's communication series. Crisis communications: A casebook approach.* Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc.

Fearn-Banks, K. (2001): "Crisis communication: A review of some best practices". In Heath, R. L., *Handbook of Public Relations* (pp. 479-485). Thousand Oaks: Sage Publications.

Fearn-Banks, K. (2002). *Crisis Communications: A Casebook Approach* (2nd ed.). Laurence Erlbaum & Associates.

Financial Post (March 26, 2018). Facebook has lost $70 billion in 10 days — and now advertisers are pulling out. Retrieved from https://business.financialpost.com/technology/u-s-ftc-investigating-facebooks-privacy-practices

Freberg, K. (2012). Intention to comply with crisis messages communicated via social media. *Public Relations Review, 38*(3), 416-421. http://dx.doi.org/10.1016/j.pubrev.2012.01.008

Gillespie, N., Hurley, R., Dietz, G., & Bachmann, R. (2012). Restoring institutional trust after the global financial crisis: A systemic approach. In Kramer, R. & Pittinsky, T. *Restoring Trust in Organizations and Leaders: Enduring Challenges and Emerging Answers*. Oxford: Oxford University Press. Pp. 185-216.

González-Herrero, A. & Smith, S. (2008). Crisis communications management on the web: How interned-based technologies are changing the way public relations professionals handle business crises. *Journal of Contingencies and Crisis Management, 16* (3), 143-153.

Gounaris, S.P. (2005). Trust and commitment influences on customer retention: insights from business-to-business services. *Journal of Business Research, 58,*126-140.

Gruber, D., Smerek, R., Thomas-Hunt, M., & James, E. (2015). The real-time power of twitter: crisis management and leadership in an age of social media. *Business Horizons*. http://dx.doi.org/10.1016/j.bushor.2014.10.006

Hagar, C. (2007). The information needs of farmers and use of ICTs. In B. Nerlich, & M. Doring (Eds.) *From Mayhem to Meaning: Assessing the social and cultural impact of the 2001*

foot and mouth outbreak in the UK (ESRC Science in Society Programme). Manchester, UK: Manchester University Press.

Hale, J., Dulek, R., & Hale, D. (2005). Crisis response communication challenges building theory from qualitative data. *Journal of Business Communication, 42*(2), 112-134. http://dx.doi.org/10.1177/0021943605274751

Halliburton, C., & Poenaru, A. (2010). The role of trust in consumer relationships. Retrieved from http://news.pb.com/white-papers/the-role-of-trust-in-consumer-relationships--escp.download

Hardin, R. 2002. *Trust and Trustworthiness.* New York: Russell Sage Foundation.

Heath, R. L. and Coombs, W.T. (2006). *Today's Public Relations: An Introduction.* Sage Publications, Inc.

Hite J. (2005). Evolutionary processes and paths of relationally embedded network ties in emerging entrepreneurial firms. *Entrepreneurship Theory and Practice, 29*, 113-144.

Hope, Maricruz, J., Khan, G., Nat, Adhikary, A. D., Pham, G. (2017, April 22). Difference Between Customer and Consumer (with Comparison Chart). Retrieved from https://keydifferences.com/difference-between-customer-and-consumer.html

Horn, I., Taros, T., Dirken, S., Hüer, L., Rose, M., Tietmeyer, R., and Constantinides, E. (2015). Business reputation and social media: A primer on threats and responses. *Journal of Direct Data and digital marketing practice* 16(3). http://dx.doi:10.1057/dddmp.2015.1

Identity Theft Resource Centre (August 31, 2018). 2018 Data breaches category summary. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2018/07/ITRC-Breach-Stats-Report-Summary-Y-T-D-2018.pdf

Ingram, T. N., Raymond W. L., Ramon A. A., Charles H. S., & Williams, M. R. (2007). *Professional Selling: A Trust-Based Approach,* 4th ed., Mason, OH: South-Western.

Jin, Y., Liu, B. F., & Austin, L. L. (2014). Examining the role of social media in effective crisis management: the effects of crisis origin, information form, and source on publics' crisis responses. *Communication Research,* 41(1), 74-94. http://dx.doi.org/10.1177/0093650211423918

Johansen, Winni and Finn Frandsen. (2007). *Krisekommunikation: Når virksomhedens image og omdømme er truet.* Frederiksberg: Forlaget Samfundslitteratur.

Jordan-Meier, J. (2011). *The four stages of highly effective crisis management: How to manage the media in the digital age.* Boca Raton, FL: CRC Press.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), 59-68.

Kernis, M. H. (2003). Toward a conceptualization of optimal self-esteem. *Psychological Inquiry*, 14: 1-26.

KPMG (Klynveld Peat Marwick Goerdeler) (2018). Me, my life, my wallet. Retrieved from https://advisory.kpmg.us/content/dam/advisory/en/pdfs/me-my-life-my-wallet-2018.pdf

Kuehner-Hebert, K. (2009). Citi imposes cut-off for IOUs. *American Banker,* 174(137), 12.

Lai, L. S., & Turban, E. (2008). Groups formation and operations in the web 2.0 environment and social networks. *Group Decision and Negotiation,17*(5), 387-402. Doi:10.1007/s10726-008-9113-2

Lewicki, R.J., McAllister, D.J., & Bies, R.J. (1998). Trust and distrust: New relationships and realities. *The Academy of Management Review, 23*(3), 438-458.

Lewis, J. D. & Weigert, A. J. (1985a). Trust as a social reality. *Social Forces,* 63, 967-985.

Lindskold, S. (1978). Trust development, the GRIT proposal, and the effects of conciliatory acts on conflict and cooperation. *Psychological Bulletin, 85*(4), 772-793. Doi:10.1037//0033-2909.85.4.772

Liu, B.F., Jin, Y., Briones, R.L. and Kuch, B. (2012). Managing turbulence online: Evaluating the blog-mediated crisis communication model with the American Red Cross. *Journal of Public Relations Research*, *24*, 353–370.

Lyons, B. and Mehta, J. (1997). Contracts, opportunism and trust: Self-interest and social orientation. *Cambridge Journal of Economics*, *21*(2), 239-257.

Mayer, R. C., Davis, J.H., & Schoorman, D. (1995). An integrative model of organizational trust, *Academy of Management Review*, *20*(3), 709–734.

McAllister, D. J. (1995). Affect and Cognitive-based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of Management Journal*, *38* (1), 24-59.

McKenzie, S. (2018, March 25). Facebook's Zuckerberg says sorry in full-page newspaper ads. CNN. Retrieved from https://www.cnn.com/2018/03/25/europe/facebook-zuckerberg-cambridge-analytica-sorry-ads-newspapers-intl/index.html

McMillan, J. H., & Schumacher, S. (2010). *Research in education: Evidence-based inquiry* (7th ed.). Boston: Pearson.

Mei, J.S.A., Bansal, N. & Pang, A. (2010). New media: a new medium in escalating crises? *Corporate Communications*,*15*(2), 143-155.

Merriam S. B. (2009). *Qualitative research: A guide to design and implementation.* 3rd ed. San Francisco, CA: Jossey-Bass.

Mitroff, I. I. 1994. Crisis management and environmentalism: A natural fit. *California Management Review*, 36(2), 101-113.

Mitroff, I. I., & Anagnos, G. (2001). *Managing crises before they happen: What every executive and manager needs to know about crisis management*. New York: AMACOM.

Murray, B. (2007). Brands must listen to web chatter. *Strategic Communication Management 11*(5), 9.

Ndubisi, N. O. (2007). Relationship marketing and customer loyalty. *Marketing Intelligence & Planning, 25*(1), 98-106. Doi:10.1108/02634500710722425

New York Times (March 17, 2018). How Trump consultants exploited the Facebook data of millions. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

New York Times (April 11, 2018). Mark Zuckerberg testimony: Day 2 brings tougher questioning. Retrieved from https://www.nytimes.com/2018/04/11/us/politics/zuckerberg-facebook-cambridge-analytica.html

New York Time (November 15, 2018). 'No Morals': Advertisers React to Facebook Report. Retrieved from https://www.nytimes.com/2018/11/15/business/media/facebook-advertisers.html

OECD (2018). Data security and privacy. Retrieved from http://www.oecd.org/going-digital/topics/digital-security-and-privacy/

Oldfield, N. C. (2017). *The power of trust: How top companies build, manage and protect it*. Success Through Trust: Halifax, N.S.

Ott, L. & Theunissen, P. (2015). Reputations at risk: engagement during social media crises. *Public Relations Review*, *41*(1), 97-102. http://dx.doi.org/10.1016/j.pubrev.2014.10.015

Paine, K. D. (2003). Guidelines for Measuring Trust 072905. *Institute for Public Relations*. Retrieved from https://instituteforpr.org/wp-content/uploads/2003_MeasuringTrust.pdf

Palen, L. & Anderson, K.M. (2016). Crisis informatics—New data for extraordinary times. *Science*, *353*, 224–225, https://doi.org/10.1126/science.aag2579

Paliszkiewicz, J. O. (2010). Organizational trust: A Critical Review of the Empirical Research. *Presented at International Conference on Technology Innovation and Industrial Management,* 16– 18 June, Pattaya, Thailand.

Park, J., Cha, M., Kim, H., & Jeong, J. (2012). Managing bad news in social media: A case study on Domino's pizza crisis (Paper presented at the ICWSM, Dublin).

Pearson, C. (2002). A blueprint for crisis management. *Ivey Business Journal,* 66(3), 69-76.

Pearson, C.M. and Clair, J.A. (1998) Reframing crisis management. *Academy of Management Review, 23*, 59-76.

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *Academy of Management Executive, 7*(1), 48-59.

Pew Research Centre (March 1, 2018). Social media use in 2018. Retrieved from http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Pew Research Centre (Sept 5, 2018). Americans are changing their relationship with Facebook. Retrieved from http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Pierson, C. T. (2009). Data breaches highlight the importance of privacy. *Financial Executive 25*(2), 62-63.

Pirson, M. & Malhotra, D. (2011). Foundations of organizational trust: What matters to different stakeholders? *Organizational Science*, 22(4), 1087-1104 http://dx.doi.org/10.1287/orsc.1100.0581

Porras, S. T. (2004). Trust as networking knowledge: Precedents from Australia. *Asia Pacific Journal of Management, 21*(3), 345–63.

Pownall, C. (2016). How social media impacts crisis communication. Retrieved from https://www.business2community.com/crisis-management/social-media-impacts-crisis-communications-01641685

PWC (PriceWaterHouseCoopers) (2017). How consumers see cybersecurity and privacy risks and what to do about it. Retrieved from https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf

Quartz (April 4, 2018). Want to change Facebook? Don't delete your account, use it for good. Retrieved from https://qz.com/1244750/the-delete-facebook-movement-is-ultimately-self-defeating/

Regester, M. & Larkin, J. (2005). *Risk issues and crisis management: A casebook of best practice.* London: Kogan Page. 3rd. ed.

Richards, C., Lawrence, G., & Burch, D. (2011). Supermarkets and Agro-industrial Foods. *Food, Culture & Society,14*(1), 29-47. Doi:10.2752/175174411x12810842291146

Rivertz (2019). Two- Factor authentication: Pain and perks. Retrieved from https://rivetz.com/2fa-study

Rooy, D. V., and Bus, J. (2010). Trust and privacy in the future internet- a research perspective. *Identity in the Information Society, 3*(2), 397-404. http://doi.org/10.1007/s12394-010-0058-7

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist, 26*, 443-452.

Schultz, F., Utz, S., & Go€ritz, A. (2011). Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media. *Public Relations Review, 37*(1), 20-27. http://dx.doi.org/10.1016/j.pubrev.2010.12.001

Scott, D. M. (2015). The new rules of marketing & PR: How to use social media, online video, mobile applications, blogs, news releases, and viral marketing to reach buyers directly, 337-350. Doi:10.1002/9781119172499.ch19

Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (1998). Communication, organization and crisis. In M. E. Roloff (Ed.), *Communication Yearbook 21*. Thousand Oaks, CA: Sage.

Selltiz, C., Wrightman, L.S., & Cook, S.W. (1976). *Research Methods in Social Relations*, Third Edition. New York: Holt, Rinehart & Winston.

Shapiro, S. P. (1987). The social control of impersonal trust. *American Journal of Sociology*, *93*, 623-658.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations.* New York, New York: Penguin Group.

Singh, J. & Sirdeshmukh, D. (2000). Agency and trust mechanisms in customer satisfaction and loyalty judgements. *Journal of the Academy of Marketing Science*, *28* (1), 150-67.

Social Media Lab. (2018). The State of Social Media in Canada 2017: A New Report From @SMLabTO Retrieved from https://socialmedialab.ca/2018/02/25/state-of-social-media-in-canada/

Solis, B. (2008). Reinventing crisis communications for the social web. Retrieved from: http://www.briansolis.com/2008/11/reinventing-crisis-communications-for/

Stephens, K.K., & Malone, P. (2012). New media for crisis communication: Opportunities for technical translation, dialogue, and stakeholder responses (pp. 381-395). In W.T. Coombs & S.J. Holladay (Eds.), *The Handbook of Crisis Communication*. West Sussex: Wiley-Blackwell.

Sturges, D.L. (1994). Communicating through crisis: A strategy for organizational survival. *Management Communication Quarterly*, *7*(3), 297–316.

Techcrunch (April 6, 2018). Facebook retracted Zuckerberg's messages from recipients' inboxes. Retrieved from https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/

Techpinions (April 11, 2018). US consumers want more transparency from Facebook. Retrieved from https://techpinions.com/us-consumers-want-more-transparency-from-facebook/52653

Tejumaiye, A. (2003). *Mass communication research: Introduction.* Lagos: Sceptre Print Limited.

The Guardian (March 17, 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

The Guardian (July 25, 2018). Facebook stocks plummet more than 20% amid concerns over growth. Retrieved from https://www.theguardian.com/technology/2018/jul/25/facebook-stocks-second-quarter-revenue-user-growth

The Statistical Portal (2018). Number of active Facebook users worldwide as of second quarter 2018. Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Ulmer, R. (2001). Effective crisis management through established stakeholder relationships: Malden Mills as a case study. *Management Communication Quarterly*, *14*(4), 590-615.

United Nations Declaration for Human Rights. Retrieved from http://www.un.org/en/universal-declaration-human-rights/index.html

USA today (March 25, 2018). Zuckerberg takes out ads to apologize as Facebook data misuse crisis intensifies. Retrieved from https://www.usatoday.com/story/tech/2018/03/25/zuckerberg-takes-out-ads-apologize-facebook-data-misuse-crisis-intensifies/456953002/

Veil, S.R., Sellnow, T.L. and Petrun, E.L. (2012a). Hoaxes and the paradoxical challenges of restoring legitimacy: Dominos' response to its YouTube crisis. *Management Communication Quarterly*, *26*(2), 322–345.

Veil, S.R. and Yang, A. (2012b). Media manipulation in the Sanlu milk contamination Crisis. *Public Relations Review*, *38*(5), 935–937.

Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A work in process literature review: incorporating social media in risk and crisis communication. *Journal of Contingencies and Crisis Management*, *19*(2), 110-122. http://dx.doi.org/10.1111/j.1468-5973.2011.00639.x

Vogelgesang, G. R. (2008). How leader interactional transparency can impact follower psychological safety and role engagement. Retrieved from http://digitalcommons.unl.edu/dissertations/AAI3291604

Walden, G. (May 14, 2018). House committees seeks input from tech CEOs. San Francisco Chronicles. Retrieved from https://www.sfchronicle.com/opinion/openforum/article/House-committee-seeks-input-from-tech-CEOs-12914113.php

Wall Street Journal (March 23, 2018). Facebook tries to calm advertisers after Cambridge Analytica Crisis. Retrieved from https://www.wsj.com/articles/facebook-tries-to-calm-advertisers-after-cambridge-analytica-crisis-1521836823

Ward, C. (2011). *Social media and crisis communication: Are organizations using social media in times of crisis?* Ball State University, Indiana.

We are social (January 30, 2018). Digital in 2018: World's internet users pass 4 billion users. Retrieved from https://wearesocial.com/blog/2018/01/global-digital-report-2018

Whetten, D.A. and Mackey, A. (2002) A social actor conception of organizational identity and its implications for the study of organizational reputation. *Business & Society*, 41(4), 393-414. http://dx.doi.org/10.1177/0007650302238775

Xia, L. (2013). Effects of companies' responses to consumer criticism in social media. *International Journal of Electronic Commerce, 17*(4), 73-100. doi:10.2753/jec1086-4415170403

Yamagishi, T., & Yamagishi, M. (1994). Trust and commitment in the United States and Japan. *Motivation and Emotion, 18*(2), 129-166. doi:10.1007/bf02249397

Yang, S. & Kang, M. (2015). . *Journal of Public Relations Research,* 27, 175-192.

Zand, D. E. (1997). *The Leadership Triad, Knowledge, Trust and Power.* New York: Oxford University Press.

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems, 86*, 914-925. doi:10.1016/j.future.2016.10.007

Zhu, W., Newman, A., Miao, Q., & Hooke, A. (2013). Revisiting the mediating role of trust in transformational leadership effects: Do different types of trust make a difference? *The Leadership Quarterly. 24*(1), 94-105.

Appendix A: INFORMED CONSENT

Dear participants,

My name is Adefolake Adedeji, and I am currently enrolled in the Master of Arts in Communication program at the Mount Saint Vincent University in Halifax, Nova Scotia. As part of my degree requirements, I am conducting research for my thesis on the impact of the privacy breach crisis on Facebook users and its effect on organizational trust.

To conduct this research, I am seeking participants who are nineteen years old and older, and who are or were Facebook users. You will be asked to complete some short measures that require checking the appropriate response box. This survey will question you regarding your views, impressions and trust in Facebook after the breach of data privacy crisis.

It is important that you as a participant fully understand how this study will be conducted, as well as any risks and/or benefits. Please note that:

This survey will require approximately **10 to 15 minutes to complete**.

- You may skip any questions you do not wish to answer, and you can **withdraw from the survey** at any time.
- You will remain **anonymous**. The information will be used for descriptive purposes only and individual participant responses will not be identified and in any way linked to the participants.
- Data collected through this survey will be stored on password-protected computer servers located in Canada. Only the researchers will have access to the data, which will be destroyed after the study is completed.
- **Respondents are not being tracked in any way**. Therefore, no one will know, whether or not you have participated in this research.
- In return for assisting us with our research we will be happy to provide you with a summary of our research results. You can send an email to adefolake.adedeji1@msvu.ca requesting access to the results. Your email request cannot be linked back to your survey responses, thereby protecting your confidentiality. The results of this study will be shared with the academic community through the presentations of this study results.

I hope that you will agree to complete this survey. If you have any questions about this research, please contact my supervisor, Dr. Alla Kushniryk, via email at alla.kushniryk@msvu.ca or via telephone at (902) 457-5070. Or, if you would like to speak to someone at arm's length from this survey, please contact the Chair of the University Research Ethics Board, via email at research@msvu.ca, or via telephone at (902) 457-6350.

Please proceed to the questionnaire if you agree to participate in this study. [*Paper version*]

Please click "NEXT" to proceed to the questionnaire if you agree to participate in this study. [*Online version*]

Appendix B: QUESTIONNAIRE

Instructions: Please put a tick ☑ in the box next to the answer of your choice.

1. Age

   ☐ 19-25

   ☐ 26-35

   ☐ 36-45

   ☐ 46-54

   ☐ 55 and above

2. Sex

   ☐ Female

   ☐ Male

   ☐ Other

3. What is your status in Mount Saint Vincent University?

   ☐ Student

   ☐ Faculty

   ☐ Other

4. If you are a student, are you in the public relations or communication programs?

   ☐ Yes ☐ No

5. How much time do you spend on Facebook daily?

   ☐ 0-1 hour

   ☐ 2-4 hours

   ☐ 5-7 hours

- ☐ 8 hours and more

6. After you learnt about the privacy breach, what did you do?

   - ☐ I stopped using Facebook
   - ☐ I adjusted my privacy setting
   - ☐ I started using Facebook less
   - ☐ Nothing Changed
   - ☐ I started using other social media platforms more
   - ☐ I have never heard about it

7. Did you participate in the #deleteFacebook campaign and deleted your Facebook account?

   - ☐ Yes, I participated and deleted
   - ☐ Yes, I participated and did not delete
   - ☐ No, I did not participate
   - ☐ I never heard about it

On a scale 1-7, where 1= strongly disagree, 2=disagree, 3=somewhat disagree, 4= neither, 5= somewhat agree, 6= agree and 7= strongly agree, DK= don't know, please indicate the extent to which you agree or disagree with each of the following statements. Please circle the appropriate response for each item:

		Strongly Disagree	Disagree	Somewhat Disagree	Neither	Somewhat Agree	Agree	Strongly Agree	Don't Know
8	I know everything about the Facebook breach of data privacy that happened in March 2018	1	2	3	4	5	6	7	DK

		Strongly Disagree	Disagree	Somewhat Disagree	Neither	Somewhat Agree	Agree	Strongly Agree	Don't Know
9	Facebook pays attention to what the users say.	1	2	3	4	5	6	7	DK
10	Facebook is timely in providing information to users.	1	2	3	4	5	6	7	DK
11	Facebook shares all necessary information with its users.	1	2	3	4	5	6	7	DK
12	Facebook is honest in communicating with its users.	1	2	3	4	5	6	7	DK
13	Facebook is transparent in sharing the organization's intent.	1	2	3	4	5	6	7	DK
14	Facebook's messages are always easy to understand.	1	2	3	4	5	6	7	DK
15	Facebook fixes every mistake it makes.	1	2	3	4	5	6	7	DK
16	Facebook keeps its promises to the users.	1	2	3	4	5	6	7	DK
17	Facebook does not care about acting ethically.	1	2	3	4	5	6	7	DK
18	When Facebook makes an important decision, it considers the impacts of the decision on the publics.	1	2	3	4	5	6	7	DK
19	I trust Facebook.	1	2	3	4	5	6	7	DK
20	Facebook acts in its users' best interest.	1	2	3	4	5	6	7	DK
21	Mark Zuckerberg, the CEO and founder of Facebook has integrity.	1	2	3	4	5	6	7	DK
22	Mark Zuckerberg is trustworthy.	1	2	3	4	5	6	7	DK
23	Mark Zuckerberg will not intentionally lie to increase Facebook's profit.	1	2	3	4	5	6	7	DK
24	Mark Zuckerberg accepts accountability for his actions.	1	2	3	4	5	6	7	DK
25	Mark Zuckerberg is proactive in righting Facebook's wrong.	1	2	3	4	5	6	7	DK
26	Mark Zuckerberg is reliable.	1	2	3	4	5	6	7	DK
27	Facebook is not respectful of privacy laws.	1	2	3	4	5	6	7	DK
28	Breach of data privacy is an important crisis.	1	2	3	4	5	6	7	DK
29	Breach of data privacy has become very common, so I have accepted that it will happen.	1	2	3	4	5	6	7	DK
30	I have confidence in how Facebook uses my data	1	2	3	4	5	6	7	DK
31	Facebook's breach of data privacy crisis has affected the trust I have in Facebook negatively.	1	2	3	4	5	6	7	DK

		Strongly Disagree	Disagree	Somewhat Disagree	Neither	Somewhat Agree	Agree	Strongly Agree	Don't Know
32	I still trust Facebook in spite of the privacy breach.	1	2	3	4	5	6	7	DK
33	Facebook intentionally sells my data.	1	2	3	4	5	6		DK
34	The way a crisis is handled has an impact on how I view the organization.	1	2	3	4	5	6	7	DK
35	Facebook responded to the privacy breach accusation five days after it was first reported. This is an appropriate amount of time.	1	2	3	4	5	6	7	DK
36	Facebook's privacy crisis could have been avoided.	1	2	3	4	5	6	7	DK
37	The way Facebook handled the crisis has restored my trust in them.	1	2	3	4	5	6	7	DK
38	I believe the information Facebook gave in regard to the privacy breach crisis is genuine and complete	1	2	3	4	5	6	7	DK
39	Facebook has taken care of every loose end and another breach of data privacy will not happen.	1	2	3	4	5	6	7	DK
40	I read privacy terms before signing up on social media.	1	2	3	4	5	6	7	DK
41	I have no problem putting my personal information (such as location and activities) on social media.	1	2	3	4	5	6	7	DK
42	Breach of data privacy is at the top of my concern when using social media.	1	2	3	4	5	6	7	DK
43	I am not concerned about what my data is used for on social media as long as I am able to connect with people.	1	2	3	4	5	6	7	DK
44	I trust an organization that uses social media to address its issues more than one who does not.	1	2	3	4	5	6	7	DK
45	A swift response by an organization on social media during a crisis contributes to restoring the trust I have in them.	1	2	3	4	5	6	7	DK
46	Facebook's detailed response to the crisis is more important than a swift response.	1	2	3	4	5	6	7	DK

Appendix C: FREQUENCY TABLES

I know everything about the Facebook breach of data privacy that happened in March 2018		
strongly disagree (1)	33	10.58%
disagree (2)	76	24.36%
somewhat disagree (3)	54	17.31%
neither (4)	18	5.77%
somewhat agree (5)	61	19.55%
agree (6)	28	8.97%
strongly agree (7)	22	7.05%
Don't Know (8)	20	6.41%

Facebook pays attention to what the users say.		
strongly disagree (1)	21	6.73%
disagree (2)	70	22.44%
somewhat disagree (3)	101	32.37%
neither (4)	21	6.73%
somewhat agree (5)	42	13.46%
agree (6)	15	4.81%
strongly agree (7)	17	5.45%
Don't Know (8)	25	8.01%

Facebook is timely in providing information to users.		
strongly disagree (1)	30	9.62%
disagree (2)	79	25.32%
somewhat disagree (3)	69	22.12%
neither (4)	28	8.97%
somewhat agree (5)	50	16.03%
agree (6)	13	4.17%
strongly agree (7)	7	2.24%
Don't Know (8)	36	11.54%

Facebook shares all necessary information with its users		
strongly disagree (1)	42	13.46%
disagree (2)	77	24.68%
somewhat disagree (3)	86	27.56%
neither (4)	19	6.09%
somewhat agree (5)	44	14.10%
agree (6)	13	4.17%
strongly agree (7)	3	0.96%
Don't Know (8)	28	8.97%

Facebook is honest in communicating with its users.		
strongly disagree (1)	27	8.65%
disagree (2)	96	30.77%
somewhat disagree (3)	95	30.45%
neither (4)	16	5.13%
somewhat agree (5)	30	9.62%
agree (6)	14	4.49%
strongly agree (7)	1	0.32%
Don't Know (8)	33	10.58%

Facebook is transparent in sharing the organization’s intent		
strongly disagree (1)	37	11.86%
disagree (2)	90	28.85%
somewhat disagree (3)	84	26.92%
neither (4)	21	6.73%
somewhat agree (5)	36	11.54%
agree (6)	11	3.53%
strongly agree (7)	2	0.64%
Don't Know (8)	31	9.94%

Facebook's messages are always easy to understand.		
strongly disagree (1)	8	2.56%
disagree (2)	56	17.95%
somewhat disagree (3)	63	20.19%
neither (4)	25	8.01%
somewhat agree (5)	70	22.44%
agree (6)	56	17.95%
strongly agree (7)	14	4.49%
Don't Know (8)	20	6.41%

Facebook fixes every mistake it makes.		
strongly disagree (1)	30	9.62%
disagree (2)	84	26.92%
somewhat disagree (3)	85	27.24%
neither (4)	14	4.49%
somewhat agree (5)	49	15.71%
agree (6)	12	3.85%
strongly agree (7)	2	0.64%
Don't Know (8)	36	11.54%

Facebook keeps its promises to the users.		
strongly disagree (1)	13	4.17%
disagree (2)	83	26.60%
somewhat disagree (3)	87	27.88%
neither (4)	28	8.97%
somewhat agree (5)	43	13.78%
agree (6)	14	4.49%
strongly agree (7)	3	0.96%
Don't Know (8)	41	13.14%

Facebook does not care about acting ethically.		
strongly disagree (1)	4	1.28%
disagree (2)	25	8.01%
somewhat disagree (3)	50	16.03%
neither (4)	28	8.97%
somewhat agree (5)	86	27.56%
agree (6)	64	20.51%
strongly agree (7)	26	8.33%
Don't Know (8)	29	9.29%

When Facebook makes an important decision, it consider the impacts of the decision on the publics.		
strongly disagree (1)	14	4.49%
disagree (2)	69	22.12%
somewhat disagree (3)	105	33.65%
neither (4)	25	8.01%
somewhat agree (5)	43	13.78%
agree (6)	21	6.73%
strongly agree (7)	5	1.60%
Don't Know (8)	30	9.62%

I trust Facebook		
strongly disagree (1)	65	20.83%
disagree (2)	108	34.62%
somewhat disagree (3)	50	16.03%
neither (4)	28	8.97%
somewhat agree (5)	34	10.90%
agree (6)	13	4.17%
strongly agree (7)	1	0.32%
Don't Know (8)	13	4.17%

Facebook acts in its users' best interest.		
strongly disagree (1)	28	8.97%
disagree (2)	68	21.79%
somewhat disagree (3)	113	36.22%
neither (4)	29	9.29%
somewhat agree (5)	37	11.86%
agree (6)	13	4.17%
strongly agree (7)	0	0.00%
Don't Know (8)	24	7.69%

Mark Zuckerberg, the CEO and founder of Facebook has integrity.		
Strongly Disagree (1)	14	4.49%
Disagree (2)	66	21.15%
Somewhat Disagree(3)	95	30.45%
Neither (4)	36	11.54%
Somewhat Agree (5)	41	13.14%
Agree (6)	20	6.41%
Strongly Agree (7)	7	2.24%
Don't Know (8)	33	10.58%

Mark Zuckerberg is trustworthy.		
Strongly Disagree (1)	22	7.05%
Disagree (2)	75	24.04%
Somewhat Disagree(3)	89	28.53%
Neither (4)	37	11.86%
Somewhat Agree (5)	36	11.54%
Agree (6)	16	5.13%
Strongly Agree (7)	3	0.96%
Don't Know (8)	34	10.90%

Mark Zuckerberg will not intentionally lie to increase Facebook's profit.		
Strongly Disagree (1)	38	12.18%
Disagree (2)	76	24.36%
Somewhat Disagree(3)	77	24.68%
Neither (4)	27	8.65%
Somewhat Agree (5)	31	9.94%
Agree (6)	14	4.49%
Strongly Agree (7)	4	1.28%
Don't Know (8)	45	14.42%

Mark Zuckerberg accepts accountability for his actions.		
Strongly Disagree (1)	14	4.49%
Disagree (2)	59	18.91%
Somewhat Disagree(3)	72	23.08%
Neither (4)	25	8.01%
Somewhat Agree (5)	67	21.47%
Agree (6)	29	9.29%
Strongly Agree (7)	5	1.60%
Don't Know (8)	41	13.14%

Mark Zuckerberg is proactive in righting Facebook’s wrong.		
Strongly Disagree (1)	13	4.17%
Disagree (2)	53	16.99%
Somewhat Disagree(3)	70	22.44%
Neither (4)	30	9.62%
Somewhat Agree (5)	66	21.15%
Agree (6)	31	9.94%
Strongly Agree (7)	5	1.60%
Don't Know (8)	44	14.10%

Mark Zuckerberg is reliable.		
Strongly Disagree (1)	20	6.41%
Disagree (2)	79	25.32%
Somewhat Disagree(3)	81	25.96%
Neither (4)	30	9.62%
Somewhat Agree (5)	40	12.82%
Agree (6)	18	5.77%
Strongly Agree (7)	2	0.64%
Don't Know (8)	42	13.46%

Facebook is not respectful of privacy laws.		
Strongly Disagree (1)	2	0.64%
Disagree (2)	17	5.45%
Somewhat Disagree(3)	42	13.46%
Neither (4)	22	7.05%
Somewhat Agree (5)	75	24.04%
Agree (6)	88	28.21%
Strongly Agree (7)	36	11.54%
Don't Know (8)	30	9.62%

Breach of data privacy is an important crisis.		
Strongly Disagree (1)	0	0.00%
Disagree (2)	3	0.96%
Somewhat Disagree(3)	4	1.28%
Neither (4)	3	0.96%
Somewhat Agree (5)	24	7.69%
Agree (6)	94	30.13%
Strongly Agree (7)	169	54.17%
Don't Know (8)	14	4.49%
No answer	1	0.32%

Breach of data privacy has become very common, so I have accepted that it will happen.		
Strongly Disagree (1)	6	1.92%
Disagree (2)	14	4.49%
Somewhat Disagree(3)	19	6.09%
Neither (4)	14	4.49%
Somewhat Agree (5)	74	23.72%
Agree (6)	90	28.85%
Strongly Agree (7)	78	25.00%
Don't Know (8)	17	5.45%

I have confidence in how Facebook uses my data.		
Strongly Disagree (1)	45	14.42%
Disagree (2)	66	21.15%
Somewhat Disagree(3)	119	38.14%
Neither (4)	20	6.41%
Somewhat Agree (5)	32	10.26%
Agree (6)	9	2.88%
Strongly Agree (7)	4	1.28%
Don't Know (8)	17	5.45%

Facebook’s breach of data privacy crisis has affected the trust I have in Facebook negatively.		
Strongly Disagree (1)	3	0.96%
Disagree (2)	22	7.05%
Somewhat Disagree(3)	30	9.62%
Neither (4)	44	14.10%
Somewhat Agree (5)	97	31.09%
Agree (6)	61	19.55%
Strongly Agree (7)	34	10.90%
Don't Know (8)	21	6.73%

I still trust Facebook in spite of the privacy breach.		
Strongly Disagree (1)	30	9.62%
Disagree (2)	72	23.08%
Somewhat Disagree(3)	92	29.49%
Neither (4)	34	10.90%
Somewhat Agree (5)	47	15.06%
Agree (6)	15	4.81%
Strongly Agree (7)	4	1.28%
Don't Know (8)	18	5.77%

Facebook intentionally sells my data.		
Strongly Disagree (1)	5	1.60%
Disagree (2)	20	6.41%
Somewhat Disagree(3)	18	5.77%
Neither (4)	25	8.01%
Somewhat Agree (5)	61	19.55%
Agree (6)	76	24.36%
Strongly Agree (7)	47	15.06%
Don't Know (8)	60	19.23%

The way a crisis is handled has an impact on how I view the organization.		
Strongly Disagree (1)	1	0.32%
Disagree (2)	6	1.92%
Somewhat Disagree(3)	6	1.92%
Neither (4)	10	3.21%
Somewhat Agree (5)	49	15.71%
Agree (6)	102	32.69%
Strongly Agree (7)	125	40.06%
Don't Know (8)	13	4.17%

Facebook responded to the privacy breach accusation five days after it was first reported. This is an appropriate amount of time.		
Strongly Disagree (1)	75	24.04%
Disagree (2)	104	33.33%
Somewhat Disagree(3)	61	19.55%
Neither (4)	9	2.88%
Somewhat Agree (5)	26	8.33%
Agree (6)	12	3.85%
Strongly Agree (7)	1	0.32%
Don't Know (8)	24	7.69%

Facebook's privacy crisis could have been avoided.		
Strongly Disagree (1)	3	0.96%
Disagree (2)	14	4.49%
Somewhat Disagree(3)	26	8.33%
Neither (4)	32	10.26%
Somewhat Agree (5)	92	29.49%
Agree (6)	67	21.47%
Strongly Agree (7)	36	11.54%
Don't Know (8)	42	13.46%

The way Facebook handled the crisis has restored my trust in them.		
Strongly Disagree (1)	20	6.41%
Disagree (2)	78	25.00%
Somewhat Disagree(3)	75	24.04%
Neither (4)	43	13.78%
Somewhat Agree (5)	38	12.18%
Agree (6)	17	5.45%
Strongly Agree (7)	2	0.64%
Don't Know (8)	39	12.50%

I believe the information Facebook gave in regard to the privacy breach crisis is genuine and complete.		
Strongly Disagree (1)	36	11.54%
Disagree (2)	84	26.92%
Somewhat Disagree (3)	65	20.83%
Neither (4)	27	8.65%
Somewhat Agree (5)	29	9.29%
Agree (6)	18	5.77%
Strongly Agree (7)	2	0.64%
Don't Know (8)	51	16.35%

Facebook has taken care of every loose end and another breach of data privacy will not happen.		
Strongly Disagree (1)	72	23.08%
Disagree (2)	90	28.85%
Somewhat Disagree(3)	65	20.83%
Neither (4)	14	4.49%
Somewhat Agree (5)	13	4.17%
Agree (6)	10	3.21%
Strongly Agree (7)	4	1.28%
Don't Know (8)	44	14.10%

I read privacy terms before signing up on social media.		
Strongly Disagree (1)	50	16.03%
Disagree (2)	73	23.40%
Somewhat Disagree (3)	82	26.28%
Neither (4)	12	3.85%
Somewhat Agree (5)	52	16.67%
Agree (6)	23	7.37%
Strongly Agree (7)	8	2.56%
Don't Know (8)	11	3.53%
No answer	0	0.00%
Not completed or Not displayed	1	0.32%

I have no problem putting my personal information (such as location and activities) on social media.		
Strongly Disagree (1)	22	7.05%
Disagree (2)	34	10.90%
Somewhat Disagree (3)	43	13.78%
Neither (4)	16	5.13%
Somewhat Agree (5)	83	26.60%
Agree (6)	70	22.44%
Strongly Agree (7)	36	11.54%
Don't Know (8)	7	2.24%
No answer	0	0.00%
Not completed or Not displayed	1	0.32%

Breach of data privacy is at the top of my concern when using social media.		
Strongly Disagree (1)	17	5.45%
Disagree (2)	46	14.74%
Somewhat Disagree (3)	95	30.45%
Neither (4)	26	8.33%
Somewhat Agree (5)	65	20.83%
Agree (6)	34	10.90%
Strongly Agree (7)	18	5.77%
Don't Know (8)	10	3.21%
Not completed or Not displayed	1	0.32%

I am not concerned about what my data is used for on social media as long as I am able to connect with people.		
Strongly Disagree (1)	35	11.22%
Disagree (2)	59	18.91%
Somewhat Disagree (3)	76	24.36%
Neither (4)	28	8.97%
Somewhat Agree (5)	61	19.55%
Agree (6)	31	9.94%
Strongly Agree (7)	11	3.53%
Don't Know (8)	10	3.21%
Not completed or Not displayed	1	0.32%

I trust an organization that uses social media to address its issues more than one who does not.		
Strongly Disagree (1)	5	1.60%
Disagree (2)	22	7.05%
Somewhat Disagree (3)	16	5.13%
Neither (4)	36	11.54%
Somewhat Agree (5)	93	29.81%
Agree (6)	77	24.68%
Strongly Agree (7)	40	12.82%
Don't Know (8)	22	7.05%
Not completed or Not displayed	1	0.32%

A swift response by an organization on social media during a crisis contributes to restoring the trust I have in them.		
Strongly Disagree (1)	1	0.32%
Disagree (2)	7	2.24%
Somewhat Disagree (3)	10	3.21%
Neither (4)	19	6.09%
Somewhat Agree (5)	85	27.24%
Agree (6)	99	31.73%
Strongly Agree (7)	69	22.12%
Don't Know (8)	21	6.73%
Not completed or Not displayed	1	0.32%

Facebook's detailed response to the crisis is more important than a swift response		
Strongly Disagree (1)	4	1.28%
Disagree (2)	26	8.33%
Somewhat Disagree (3)	42	13.46%
Neither (4)	46	14.74%
Somewhat Agree (5)	82	26.28%
Agree (6)	59	18.91%
Strongly Agree (7)	25	8.01%
Don't Know (8)	27	8.65%
Not completed or Not displayed	1	0.32%

Appendix D: MEANS and Standard Deviations

	N	Mean	Std. Deviation
Breach of data privacy is an important crisis.	297	6.39	.909
The way a crisis is handled has an impact on how I view the organization.	299	6.03	1.142
A swift response by an organization on social media during a crisis contributes to restoring the trust I have in them.	290	5.60	1.191
Breach of data privacy has become very common, so I have accepted that it will happen.	295	5.43	1.497
Facebook intentionally sells my data.	252	5.12	1.569
I trust an organization that uses social media to address its issues more than one who does not.	289	5.01	1.461
Facebook's privacy crisis could have been avoided.	270	5.00	1.392
Facebook's breach of data privacy crisis has affected the trust I have in Facebook negatively.	291	4.82	1.435
Facebook's detailed response to the crisis is more important than a swift response	284	4.60	1.485
I have no problem putting my personal information (such as location and activities) on social media.	304	4.51	1.804
I am (not) concerned about what my data is used for on social media as long as I am able to connect with people. R	301	4.48	1.676
Facebook's messages are always easy to understand.	292	4.09	1.634
Breach of data privacy is at the top of my concern when using social media.	301	3.83	1.619
Mark Zuckerberg is proactive in righting Facebook's wrong.	268	3.73	1.517
Mark Zuckerberg accepts accountability for his actions.	271	3.66	1.528
I know everything about the Facebook breach of data privacy that happened in March 2018	292	3.58	1.830
Mark Zuckerberg, the CEO and founder of Facebook has integrity.	279	3.40	1.431
Facebook pays attention to what the users say.	287	3.37	1.577
Facebook care about acting ethically. R	283	3.36	1.515

When Facebook makes an important decision, it consider the impacts of the decision on the publics.	282	3.34	1.409
The way Facebook handled the crisis has restored my trust in them.	273	3.22	1.389
Facebook keeps its promises to the users.	271	3.22	1.356
Facebook is timely in providing information to users.	276	3.20	1.531
Mark Zuckerberg is reliable.	270	3.20	1.407
I still trust Facebook in spite of the privacy breach.	294	3.19	1.433
Mark Zuckerberg is trustworthy.	278	3.18	1.379
I read privacy terms before signing up on social media.	300	3.15	1.658
Facebook acts in its users' best interest.	288	3.06	1.284
Facebook fixes every mistake it makes.	276	3.04	1.419
Facebook is respectful of privacy laws. R	282	3.02	1.470
Facebook shares all necessary information with its users.	284	2.99	1.462
Mark Zuckerberg will not intentionally lie to increase Facebook's profit.	267	2.98	1.462
I believe the information Facebook gave in regard to the privacy breach crisis is genuine and complete.	261	2.97	1.474
I have confidence in how Facebook uses my data.	295	2.90	1.350
Facebook is honest in communicating with its users.	279	2.90	1.313
Facebook is transparent in sharing the organization's intent.	281	2.89	1.377
I trust Facebook	299	2.67	1.457
Facebook responded to the privacy breach accusation five days after it was first reported. This is an appropriate amount of time.	288	2.47	1.397
Facebook has taken care of every loose end and another breach of data privacy will not happen.	268	2.45	1.391
Valid N (listwise)	207		

Appendix E: CORRELATIONS

Correlations

		Trust	Leadership	Concern for Facebook Privacy	Handling crisis	Concern for privacy on social media (a)	Trust in social media (b)
Trust	Pearson Correlation	1	.743**	-.692**	.700**	-.077	.091
	Sig. (2-tailed)		.000	.000	.000	.229	.157
	N	250	244	231	221	249	243
Leadership	Pearson Correlation	.743**	1	-.615**	.647**	-.128*	.163*
	Sig. (2-tailed)	.000		.000	.000	.041	.010
	N	244	254	233	222	253	247
Concern for Facebook Privacy	Pearson Correlation	-.692**	-.615**	1	-.818**	.231**	-.014
	Sig. (2-tailed)	.000	.000		.000	.000	.831
	N	231	233	245	217	245	237
Handling crisis	Pearson Correlation	.700**	.647**	-.818**	1	-.244**	.026
	Sig. (2-tailed)	.000	.000	.000		.000	.696
	N	221	222	217	231	231	229
Concern for privacy on social media (a)	Pearson Correlation	-.077	-.128*	.231**	-.244**	1	-.174**
	Sig. (2-tailed)	.229	.041	.000	.000		.004
	N	249	253	245	231	296	278
Trust in social media (b)	Pearson Correlation	.091	.163*	-.014	.026	-.174**	1
	Sig. (2-tailed)	.157	.010	.831	.696	.004	
	N	243	247	237	229	278	280

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Appendix F: AGE

Table 1: Descriptives

		N	Mean	Std. Deviation
I know everything about the Facebook breach of data privacy that happened in March 2018	19-25	156	3.23	1.741
	26-35	79	3.84	1.667
	36-45	26	3.54	1.985
	46-54	18	4.44	2.229
	55 and above	13	5.15	1.725
	Total	292	3.58	1.830
Trust	19-25	129	3.1428	.87321
	26-35	72	3.2581	1.07442
	36-45	21	2.8373	.77660
	46-54	16	2.9167	.93541
	55 and above	12	3.0417	1.09665
	Total	250	3.1310	.94380
Leadership	19-25	131	3.3003	1.12952
	26-35	73	3.6164	1.18102
	36-45	22	2.5455	1.13294
	46-54	15	3.1667	.97386
	55 and above	13	3.4103	1.63811
	Total	254	3.3235	1.19093
Concern for Facebook Privacy	19-25	128	5.2547	.92036
	26-35	70	5.1457	1.03443
	36-45	20	5.7100	.87172
	46-54	15	5.7467	.97531
	55 and above	12	5.8667	.96985
	Total	245	5.3208	.97414
Handling crisis	19-25	120	2.8250	.91996
	26-35	68	3.1078	1.12773
	36-45	17	2.1961	.97046
	46-54	14	2.5833	1.27894
	55 and above	12	2.1667	.82572
	Total	231	2.8131	1.03820
Concern for privacy on social media (a)	19-25	157	3.2070	1.29724
	26-35	81	3.5679	1.28635
	36-45	26	4.0000	1.46287
	46-54	19	4.1316	1.38285
	55 and above	13	4.6154	1.35637
	Total	296	3.4966	1.36419
Trust in social media (b)	19-25	145	4.8241	1.03041
	26-35	80	4.6813	1.20913
	36-45	23	4.2826	1.17334
	46-54	19	4.3421	1.20822
	55 and above	13	4.6154	1.12553
	Total	280	4.6964	1.11835

Table 2: ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
I know everything about the Facebook breach of data privacy that happened in March 2018	Between Groups	69.876	4	17.469	5.539	.000
	Within Groups	905.151	287	3.154		
	Total	975.027	291			
Trust	Between Groups	3.823	4	.956	1.074	.370
	Within Groups	217.977	245	.890		
	Total	221.800	249			
Leadership	Between Groups	20.120	4	5.030	3.698	.006
	Within Groups	338.717	249	1.360		
	Total	358.837	253			
Concern for Facebook Privacy	Between Groups	12.031	4	3.008	3.288	.012
	Within Groups	219.513	240	.915		
	Total	231.544	244			
Handling crisis	Between Groups	18.150	4	4.538	4.463	.002
	Within Groups	229.756	226	1.017		
	Total	247.906	230			
Concern for privacy on social media (a)	Between Groups	44.100	4	11.025	6.354	.000
	Within Groups	504.897	291	1.735		
	Total	548.997	295			
Trust in social media (b)	Between Groups	8.793	4	2.198	1.777	.134
	Within Groups	340.154	275	1.237		
	Total	348.946	279			

Table 3: Multiple Comparison
Turkey HSD

Dependent Variable	(I) Age	(J) Age	Mean Difference (I-J)	Std. Error	Sig.
I know everything about the Facebook breach of data privacy that	19-25	26-35	-.605	.245	.101
		36-45	-.308	.376	.925
		46-54	-1.214*	.442	.050
		55 and above	-1.923*	.513	.002
	26-35	19-25	.605	.245	.101
		36-45	.297	.402	.947

happened in March 2018		46-54	-.609	.464	.683
		55 and above	-1.318	.532	.098
	36-45	19-25	.308	.376	.925
		26-35	-.297	.402	.947
		46-54	-.906	.545	.458
		55 and above	-1.615	.603	.060
	46-54	19-25	1.214*	.442	.050
		26-35	.609	.464	.683
		36-45	.906	.545	.458
		55 and above	-.709	.646	.808
	55 and above	19-25	1.923*	.513	.002
		26-35	1.318	.532	.098
		36-45	1.615	.603	.060
		46-54	.709	.646	.808
Leadership	19-25	26-35	-.31618	.17035	.344
		36-45	.75480*	.26873	.042
		46-54	.13359	.31792	.993
		55 and above	-.11000	.33915	.998
	26-35	19-25	.31618	.17035	.344
		36-45	1.07098*	.28367	.002
		46-54	.44977	.33064	.654
		55 and above	.20618	.35110	.977
	36-45	19-25	-.75480*	.26873	.042
		26-35	-1.07098*	.28367	.002
		46-54	-.62121	.39054	.505
		55 and above	-.86480	.40801	.215
	46-54	19-25	-.13359	.31792	.993
		26-35	-.44977	.33064	.654
		36-45	.62121	.39054	.505
		55 and above	-.24359	.44196	.982
	55 and above	19-25	.11000	.33915	.998
		26-35	-.20618	.35110	.977
		36-45	.86480	.40801	.215
		46-54	.24359	.44196	.982
Concern for Facebook Privacy	19-25	26-35	.10897	.14217	.940
		36-45	-.45531	.22995	.279
		46-54	-.49198	.26100	.328
		55 and above	-.61198	.28873	.215

	26-35	19-25	-.10897	.14217	.940
		36-45	-.56429	.24248	.140
		46-54	-.60095	.27211	.180
		55 and above	-.72095	.29881	.115
	36-45	19-25	.45531	.22995	.279
		26-35	.56429	.24248	.140
		46-54	-.03667	.32666	1.000
		55 and above	-.15667	.34922	.992
	46-54	19-25	.49198	.26100	.328
		26-35	.60095	.27211	.180
		36-45	.03667	.32666	1.000
		55 and above	-.12000	.37040	.998
	55 and above	19-25	.61198	.28873	.215
		26-35	.72095	.29881	.115
		36-45	.15667	.34922	.992
		46-54	.12000	.37040	.998
Handling crisis	19-25	26-35	-.28284	.15304	.349
		36-45	.62892	.26129	.117
		46-54	.24167	.28476	.915
		55 and above	.65833	.30527	.200
	26-35	19-25	.28284	.15304	.349
		36-45	.91176*	.27341	.009
		46-54	.52451	.29592	.392
		55 and above	.94118*	.31570	.026
	36-45	19-25	-.62892	.26129	.117
		26-35	-.91176*	.27341	.009
		46-54	-.38725	.36389	.825
		55 and above	.02941	.38016	1.000
	46-54	19-25	-.24167	.28476	.915
		26-35	-.52451	.29592	.392
		36-45	.38725	.36389	.825
		55 and above	.41667	.39665	.831
	55 and above	19-25	-.65833	.30527	.200
		26-35	-.94118*	.31570	.026
		36-45	-.02941	.38016	1.000
		46-54	-.41667	.39665	.831
	19-25	26-35	-.36089	.18020	.267
		36-45	-.79299*	.27890	.038

Concern for privacy on social media (a)		46-54	-.92457*	.31995	.033
		55 and above	-1.40838*	.38015	.002
	26-35	19-25	.36089	.18020	.267
		36-45	-.43210	.29691	.592
		46-54	-.56368	.33577	.449
		55 and above	-1.04748	.39355	.062
	36-45	19-25	.79299*	.27890	.038
		26-35	.43210	.29691	.592
		46-54	-.13158	.39756	.997
		55 and above	-.61538	.44743	.644
	46-54	19-25	.92457*	.31995	.033
		26-35	.56368	.33577	.449
		36-45	.13158	.39756	.997
		55 and above	-.48381	.47411	.846
	55 and above	19-25	1.40838*	.38015	.002
		26-35	1.04748	.39355	.062
		36-45	.61538	.44743	.644
		46-54	.48381	.47411	.846

*. The mean difference is significant at the 0.05 level

Appendix G: TIME

Table 1: Descriptives

		N	Mean	Std. Deviation
I know everything about the Facebook breach of data privacy that happened in March 2018	0-1 hour	193	3.05	1.634
	2-4 hours	84	4.40	1.673
	5-7 hours	11	6.18	1.601
	8 hours and more	4	5.00	1.826
	Total	292	3.58	1.830
Trust	0-1 hour	160	3.1734	.91621
	2-4 hours	76	3.0844	.93517
	5-7 hours	11	2.7727	1.34737
	8 hours and more	3	3.3611	1.13141
	Total	250	3.1310	.94380
Leadership	0-1 hour	162	3.3868	1.10985
	2-4 hours	78	3.2628	1.29198
	5-7 hours	11	2.6667	1.46059
	8 hours and more	3	3.8889	1.41748
	Total	254	3.3235	1.19093
Concern for Facebook Privacy	0-1 hour	154	5.1870	.94797
	2-4 hours	76	5.4711	.92301
	5-7 hours	12	6.1667	.99026
	8 hours and more	3	5.0000	1.73205
	Total	245	5.3208	.97414
Handling crisis	0-1 hour	142	2.9308	1.00496
	2-4 hours	75	2.6711	.99510
	5-7 hours	11	2.2879	1.45696
	8 hours and more	3	2.7222	1.49381
	Total	231	2.8131	1.03820
Concern for privacy on social media (a)	0-1 hour	196	3.2449	1.24704
	2-4 hours	84	3.8810	1.37231
	5-7 hours	12	4.8333	1.77525
	8 hours and more	4	3.7500	1.65831
	Total	296	3.4966	1.36419
Trust in social media (b)	0-1 hour	182	4.6484	1.13762
	2-4 hours	83	4.7982	1.11082
	5-7 hours	11	4.7500	.92195
	8 hours and more	4	4.6250	1.10868

	Total	280	4.6964	1.11835

Table 2: ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
I know everything about the Facebook breach of data privacy that happened in March 2018	Between Groups	194.573	3	64.858	23.933	.000
	Within Groups	780.455	288	2.710		
	Total	975.027	291			
Trust	Between Groups	2.024	3	.675	.755	.520
	Within Groups	219.776	246	.893		
	Total	221.800	249			
Leadership	Between Groups	6.642	3	2.214	1.571	.197
	Within Groups	352.195	250	1.409		
	Total	358.837	253			
Concern for Facebook Privacy	Between Groups	13.367	3	4.456	4.922	.002
	Within Groups	218.177	241	.905		
	Total	231.544	244			
Handling crisis	Between Groups	6.537	3	2.179	2.049	.108
	Within Groups	241.369	227	1.063		
	Total	247.906	230			
Concern for privacy on social media (a)	Between Groups	46.526	3	15.509	9.012	.000
	Within Groups	502.471	292	1.721		
	Total	548.997	295			
Trust in social media (b)	Between Groups	1.332	3	.444	.353	.787
	Within Groups	347.614	276	1.259		
	Total	348.946	279			

Table 3: Multiple Comparisons

Tukey HSD

Dependent Variable	(I) How much time do you spend on Facebook daily?	(J) How much time do you spend on Facebook daily?	Mean Difference (I-J)	Std. Error	Sig.
I know everything about the Facebook breach of data privacy that happened in March 2018	0-1 hour	2-4 hours	-1.358*	.215	.000
		5-7 hours	-3.135*	.510	.000
		8 hours and more	-1.953	.832	.090
	2-4 hours	0-1 hour	1.358*	.215	.000
		5-7 hours	-1.777*	.528	.005
		8 hours and more	-.595	.842	.894

	5-7 hours	0-1 hour	3.135*	.510	.000
		2-4 hours	1.777*	.528	.005
		8 hours and more	1.182	.961	.609
	8 hours and more	0-1 hour	1.953	.832	.090
		2-4 hours	.595	.842	.894
		5-7 hours	-1.182	.961	.609
Concern for Facebook Privacy	0-1 hour	2-4 hours	-.28404	.13338	.147
		5-7 hours	-.97965*	.28517	.004
		8 hours and more	.18701	.55466	.987
	2-4 hours	0-1 hour	.28404	.13338	.147
		5-7 hours	-.69561	.29556	.089
		8 hours and more	.47105	.56007	.835
	5-7 hours	0-1 hour	.97965*	.28517	.004
		2-4 hours	.69561	.29556	.089
		8 hours and more	1.16667	.61417	.231
	8 hours and more	0-1 hour	-.18701	.55466	.987
		2-4 hours	-.47105	.56007	.835
		5-7 hours	-1.16667	.61417	.231
Concern for privacy on social media (a)	0-1 hour	2-4 hours	-.63605*	.17107	.001
		5-7 hours	-1.58844*	.39010	.000
		8 hours and more	-.50510	.66255	.871
	2-4 hours	0-1 hour	.63605*	.17107	.001
		5-7 hours	-.95238	.40483	.089
		8 hours and more	.13095	.67133	.997
	5-7 hours	0-1 hour	1.58844*	.39010	.000
		2-4 hours	.95238	.40483	.089
		8 hours and more	1.08333	.75736	.481
	8 hours and more	0-1 hour	.50510	.66255	.871
		2-4 hours	-.13095	.67133	.997
		5-7 hours	-1.08333	.75736	.481
		2-4 hours	-.04819	.36010	.999
		8 hours and more	.12500	.65526	.998
	8 hours and more	0-1 hour	-.02335	.56726	1.000
		2-4 hours	-.17319	.57449	.990
		5-7 hours	-.12500	.65526	.998

*. The mean difference is significant at the 0.05 level.

Appendix H: PR Students vs Others

Table 1: Group Statistics

	If you are a student, are you in the public relations or communication programs?	N	Mean	Std. Deviation	Std. Error Mean
I know everything about the Facebook breach of data privacy that happened in March 2018	Yes	159	3.85	1.692	.134
	No	119	2.97	1.766	.162
Facebook's detailed response to the crisis is more important than a swift response	Yes	158	4.53	1.453	.116
	No	111	4.80	1.476	.140
Breach of data privacy has become very common, so I have accepted that it will happen.	Yes	160	5.75	1.308	.103
	No	120	5.03	1.611	.147
The way a crisis is handled has an impact on how I view the organization.	Yes	161	6.13	1.056	.083
	No	123	5.86	1.270	.114
Handling crisis	Yes	145	2.8138	1.04056	.08641
	No	73	2.9269	.95581	.11187

Table 2: Independent Samples Test

		Levene's Test for Equality of Variances				
		F	Sig.	t	df	Sig. (2-tailed)
I know everything about the Facebook breach of data privacy that happened in March 2018	Equal variances assumed	.539	.463	4.224	276	.000
	Equal variances not assumed			4.198	248.341	.000
Facebook's detailed response to the crisis is more important than a swift response	Equal variances assumed	.365	.546	-1.527	267	.128
	Equal variances not assumed			-1.522	234.570	.129

Breach of data privacy has become very common, so I have accepted that it will happen.	Equal variances assumed	2.701	.101	4.153	278	.000
	Equal variances not assumed			4.032	224.629	.000
The way a crisis is handled has an impact on how I view the organization.	Equal variances assumed	4.040	.045	1.946	282	.053
	Equal variances not assumed			1.898	234.917	.059
Handling crisis	Equal variances assumed	.137	.711	-.778	216	.437
	Equal variances not assumed			-.800	155.818	.425