# Data leaks

*An investigation of a new cybersecurity crisis and its results on post-crisis reputation and users' engagement on social media.*

**Student Name:** Christina Sideri

**Student Number:** 510896

**Supervisor:** Dr. Yijing Wang

**Media and Business**

**Erasmus School of History, Culture and Communication**

**Erasmus University Rotterdam**

**Master Thesis**

*June 27, 2019*

**Data leaks:** an investigation of a new cybersecurity crisis and its results on post-crisis reputation and users' engagement on social media.


## Abstract

Cybersecurity has become a significant reality in modern societies, as people provide their intimate and personal information to the digital space. This data can be proved very useful for the companies themselves, but, without a doubt, cybersecurity attacks and data leaks are a new type of crisis that companies are forced to take into consideration. From an academic perspective, data leaks and their effect on the reputation of the companies is a topic that has not been examined in depth by scholars and thus, the aim of this study was to add value in the crisis communication field by examining this new type of crisis. In addition, this research attempted to analyze this crisis within the context of social media, as they also constitute a new reality for crisis communication.

Drawing upon the Situational Crisis Communication theory and the Social Mediated Crisis Communication theory, the present study tried to identify whether the crisis responsibility, the pre-crisis reputation and the CEO's credibility can influence the reputation of an organization after a data leak incident. Taking the Facebook - Cambridge Analytica scandal as an example, a digital survey was formulated and disseminated to Facebook users globally. The results of the 155 respondents indicated that crisis responsibility and pre-crisis reputation can have a significant effect on the reputation of an organization after a cybersecurity incident. Most importantly, this research proved that the CEO's credibility is a significant predictor of the post-crisis reputation of an organization, but unfortunately, no predictors of Secondary Crisis Communications were found significant in this study.

The outcomes of the research imply the extension of the SCCT model to the cybersecurity crises, as well as the addition of the CEO's credibility as an indicator of the post-crisis reputation of the organization. Next to this, the managerial and theoretical implications are provided in the last section of the study. To conclude, recommendations for future research urge scholars to dive into the examination of the complete model of

SCCT theory within the context of data leaks but most importantly to identify the predictors of the public's engagement on social media after a crisis, since it is proved to be detrimental and unpredicted so far.

**Key Words:** Crisis Communication, Cyber Security, Crisis Responsibility, CEO Credibility, Pre-Crisis Reputation, Post-Crisis Reputation, Secondary Crisis Communications

**Abbreviations**

| | | |
|---|---|---|
| CEO | – | Chief Executive Officer |
| EFA | – | Exploratory Factor Analysis |
| eWOM | – | electronic Word of Mouth |
| IV | – | Independent Variable |
| KMO | - | Kaiser-Meyer-Olkin |
| PII | – | Personal Identifiable information |
| SCCT | - | Situational Crisis Communication Theory |
| SD | – | Standard Deviation |
| SMCC | – | Social Mediated Crisis Communication |

# Table of Contents

## 1.Introduction

In this day and age, where technology and the use of the Internet has penetrated people's lives, radical changes can be detected in individuals' daily routine. From a global perspective, people have started to embed their daily habits and routine into the digital world, which the latter, provides them innumerable services to fulfill their needs and desires (Leung & Lee, 2005). For instance, in the cyberspace, people have the opportunity to find an array of sources about news in relation to their interest, while shopping at the stores have been replaced by e-commerce which allows individuals to buy their desirable products from every part of the world through the use of their credit card. Last but not least, social media enabled users globally to create their own profiles on the digital world and talk with their friends and family or even expand their network and make new connections (Leung & Lee, 2005). However, interaction with Websites and social media increasingly demands the provision of sensitive and essential personal information such as home address, date and place of birth, passwords and other important data (Philips, 2002; Veltsos 2012). Therefore, no matter how convenient all these practices might seem, a big question is raised: "How secure are the private life and private information of users in the digital world?".

By the year 2017, 5,418 data breach incidents have been published since 2005 with a total of nearly 1 billion records breached, affecting more than 85 million users' accounts across different industries (Identity Theft Resource Center, 2014). According to Veltsos (2012), a data breach can be characterized as a case when personal identifiable information (PII) is leaked by a third party and is related to personal information that constitute the users' identity, such as a full name, home and work address, SSN, date and place of birth, parents' full names, and biometric records (Veltsos, 2012, p. 197).

Cybersecurity has been gaining public attention as cyber-attacks such as data leaks incidents have been frequently reported in the media (Wang & Park, 2017). The case study that will be examined as an example of cybersecurity crisis in this research is Facebook – Cambridge Analytica scandal. In March 2018, The New York Times, in collaboration with The Observer of London and The Guardian, obtained an array of

documents from inside Cambridge Analytica which revealed that Cambridge Analytica had embezzled the personal data of millions of people's Facebook accounts without their permission and used it for political purposes. A great majority of the public started deleting its account, while at the same period of time, the hashtag #DeleteFacebook was trending on Twitter (Confessore, 2018). Furthermore, politicians from both the US and Britain demanded some answers from the CEO of Facebook, Mark Zuckerberg, in order to decide whether Facebook had violated an agreement regarding the safeguarding of users' personal data. Initially, Mark Zuckerberg apologized for the incident with Cambridge Analytica on CNN (Confessore, 2018) and published a personal letter to numerous newspapers and social media. Additionally, he promised to the users that Facebook will take further actions in order to prevent such a crisis in the future. However, after one month, the CEO of Facebook was called to testify in the US Congress where he had to reply to questions regarding the mishandling of users' data. Ultimately, Mark Zuckerberg took the whole responsibility of the incident. He argued that since he is the Chief Executive and owner of Facebook he had to take more strict actions in order to prevent such a crisis. This scandal has been characterized as a crucial point in the public's understanding of the misusage of its personal data and triggered a massive decrease in Facebook's stock price. As a matter of fact, it was considered the largest known data leak in history (Confessore, 2018).

Despite the extended popularity of the incident and the harm that may have caused to the victims, a recent study has indicated that Facebook still constitutes the first most used social media platform globally (Gramlich, 2019). Additionally, another research indicated that 74% of American adults still use their Facebook account at least once a day (Gramlich, 2019).

For corporations, data breaches present great threats: organizations (e.g. banks, financial institutions, health care providers) should comply with legal requirements imposed by the Federal Trade Commission as they should alert all customers – both affected and potentially affected - regarding compromised personal data. What is more, there are also ethical and legitimate responsibilities. Hence, when a crisis emerges, organizations should also inform stakeholders about the necessary steps that need to be

taken to protect themselves. According to Kim et al. (2017), data breaches have essential ramifications to a firm's image, while economic damages should not be neglected. According to research, cybercrime costed $450 dollars to the global economy only in 2016 (Graham, 2017), which makes clear how a data breach can lead to high expenditures for a company. Some of the expenses include legal guidance, scientific investigation and regulatory fines (Verizon, 2016). Nevertheless, businesses have to be aware of the much higher indirect costs that may arise, such as reputational damage and loss of customer trust (Anderson et al., 2012).

The reason for focusing specifically on the case of data breach in this study, is due to the fact that it is a relatively new type of crisis that has become a significant reality of the digital economy as it can be seen by the frequent media reports (Wang & Park, 2017). These crises may provoke detrimental ramifications to both customers and businesses and may turn into corporate crises (Wang & Park, 2017). From a social viewpoint, this study examines a highly debatable and concerning issue that exists in modern societies, which is the implications of social media privacy and the use and abuse of personal data (Wang & Park, 2017). Therefore, results could be implemented to the crisis communication strategic plan of a corporation, in order to deal with same possible crises in the future. Overall, safeguarding the reputation is an evident task every company must carry out.

Furthermore, data leaks is a type of crisis that has not been examined in depth from an academic perspective. In fact, previous academic research regarding cybersecurity attacks can be segregated into two main topics. The first theme addresses issues of syntactic cyber-attacks whose goal is to acquire valuable knowledge regarding a software or hardware (Kwang & Choo, 2011). Other studies have analyzed cyber-attacks and their impact on governments or businesses such as cyber-piracy in music or gaming (Franke & Brynielsson, 2014). Moreover, research is also focused on the effects of data breaches to organizations as well as the legal requirements that have to be implemented in order to avoid them (Kim, Johnson & Park, 2017; Ramakrishna, 2012). However, little is known regarding the embezzlement of private data through social media platforms as a form of cyber-attack, as well as its impact on the online behavior of the users, who are also considered as victims.

Therefore, the purpose of this study is to enrich the crisis communication literature by examining the effects of data breaches not only to the reputation of the corporation, but also its impact on the users' behavior on social media.

As mentioned in the literature, there is a variety of factors that can influence the reputation of an organization after a crisis. Firstly, according to Coombs (2007), the already established reputation and relationship of an organization with its customers can be considered as an instrumental determiner. Since Facebook had a favorable reputation for over a decade, this research will try to measure whether the perceptions of stakeholders regarding the reputation of the organization can be altered in the case of a cybersecurity incident and whether this crisis can affect their behavior on social media. In the literature, there is a debate whether a high reputation can be considered as an asset. On the one hand, scholars argue that a prior high reputation can protect the organization of a reputational loss (Alsop, 2004; Roberts & Dowling, 2002; Fombrun and van Riel, 2003). On the contrary, other researchers claim that an organization with a strong reputation can experience a detrimental reputational loss, as, during a crisis, the high expectations of individuals are violated (Dean, 2004; Rhee, & Haunschild, 2006; Grunwald & Hempelmann, 2011).

Moreover, the amount of the attributed blame to an organization by its stakeholders is also proved to play a significant role in its post-crisis reputation (Coombs, 2007). When a crisis emerges, stakeholders experience different emotions based on the responsibility they attribute to the organization, which in turn leads to different behavioral intentions. Therefore, when the level of responsibility for the organization is relatively high, stakeholders might feel angry and disappointed. On the other side of the spectrum, if the public doesn't put the blame on the organization, it may feel sympathy for the organization and not result on behaviors such as negative eWOM or termination of its relationship with the organization (Coombs, 2007). From the perspective of the organizations, corporations desire to know the level of the blame that is attributed to them in order to frame the situation of the crisis and proceed to the creation of the most appropriate crisis response. In the case of Facebook Cambridge Analytica scandal, the CEO of Facebook took the whole responsibility of the data breach in 2018 and

apologized for the damage it caused to its users. Therefore, it is interesting to investigate whether, in the case of data breaches in general, the amount of crisis responsibility attributed by the public actually has an impact on the post-crisis reputation of the users, as well as on their online behavior.

Last but not least, another element that can also affect the post-crisis reputation is the CEO's credibility (Treadway et al., 2009; Chen & Chun, 2007; Alghavi et al., 2014). In fact, research has shown that CEOs who are considered credible by their stakeholders, can have a positive impact on the reputation of their firms, as they are able to influence the public's opinions and perceptions of a crisis (Chen & Chun, 2007). In fact, oftentimes, CEOs are so closely related to the company they work for and thus, their reputation is closely connected with the reputation of the organization.

Based on these findings in the literature, the present research will further examine the above-mentioned concepts by using the Situational Crisis Communication Theory (SCCT) (Coombs 2007) and the SMCC theory as groundwork. The former model is essential in order to measure the pre-crisis reputation, the crisis responsibility as well as the post-crisis reputation of the organization, while the latter is significant to use in order to assess the behavioral intentions of the victims of a data breach on social media. To conclude, this research will try to enrich the academic field of crisis communication by examining whether the aforementioned variables have a significant impact in the case of a cybersecurity crisis. Thus, the following research question is proposed:

> ***RQ**: What are the impacts of the CEO's credibility, pre-crisis reputation and crisis responsibility to the organizations' post-crisis reputation and the secondary crisis communications of the users in a cybersecurity crisis?*

After having introduced the area of interest of this study as well as the research question, the second chapter presents the theoretical context and previous findings that were considered relevant and appropriate for this study. This chapter will be segmented to sub-sections in order to give a more detailed description of previous findings stated in the literature regarding the different variables that are going to be measured. Every sub-section will conclude with two hypotheses. Subsequently, the third chapter will dive into

the research design as well as the operationalization of the data analysis and the measurement of the theoretical concepts. The outcomes of the data analysis will be presented and discussed in chapter four while the following chapter will explain the managerial implications of this study. Finally, in the last section, the strengths and limitations of this thesis project will be presented and recommendations for future research will be proposed.

## 2. Theoretical framework

## Corporate Reputation Theories

### 2.1. Situational Crisis Communication Theory

This research will focus on two types of theoretical contexts. First and foremost, the Situational Crisis Communication Theory (SCCT) model will be used, which was built on the premise of Attribution theory (Weiner, 1972). The latter, suggests that when crises emerge, people seek for the underlying causes of events that happen around them and attribute blame to the involved actors in a crisis (Coombs, 2007; Weiner, 1985). Additionally, SCCT model, just like Image Repair theory (Benoit, 1997), distinguishes various response strategies. Nevertheless, the reason that only the SCCT model was chosen as a framework, is due to the fact that the SCCT model lies upon its focus on audiences. It pursues to find out how people perceive crises, what are their reactions to crisis response strategies and to the organization in a crisis (Coombs & Holladay, 2010). Additionally, it explores the crisis situation and adjusts these strategies to the corresponding frame (see Figure 1)(Coombs, 2007).

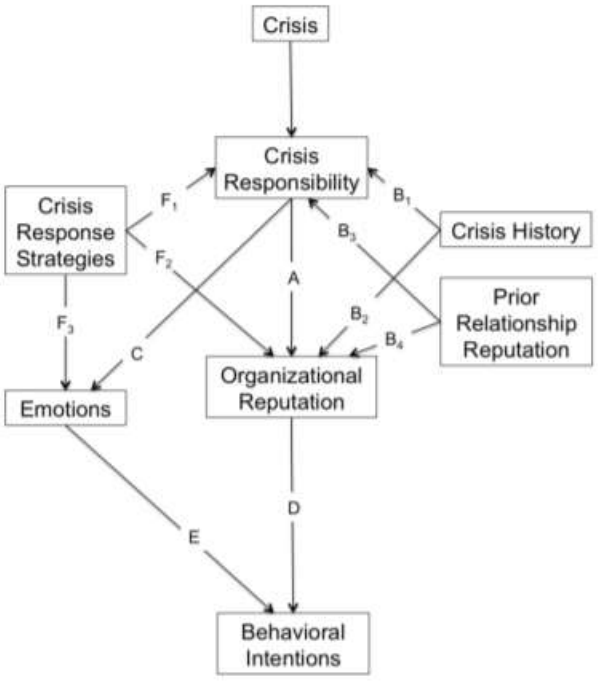


***Figure 2.1.*** *Crisis Situation model of SCCT (Coombs, 2007)*

More specifically, SCCT identifies three components that shape the reputational threat: the initial crisis responsibility, the crisis history, and the prior relational reputation. Based on the model, crisis managers should evaluate the threat to a reputation using a two-step process. To begin with, the first step is the identification and acknowledgment of the crisis type. The crises types regulate how much responsibility is attributed by stakeholders to the organization. In the SCCT model, crises types refer to the causes of a crisis which can be attributed to an external agent, by the members of the organization accidentally or intentionally, or it can be a result of technical or human error. Next, each type of crisis is allocated to a cluster. In the first cluster, victims attribute low responsibility to organizations (e.g. natural disasters) and consider the organization as a victim as well. The second cluster -the accidental cluster- has a small degree of attributed responsibility (e.g. technical-error accident) and the incident is assumed unforeseeable or uncontrollable by the organization. Last but not least, the third cluster -the intentional cluster- is comprised of high levels of attributions of crisis responsibility (e.g. human-error product harm and organizational misdeed) and the event is characterized as purposeful (Coombs and Holladay, 2002).

Moreover, the second step of the process that plays a significant role in identifying the reputational threat of a crisis, is the crisis history of the company (Coombs, 2007). Crisis history refers to whether or not an organization had experienced a similar crisis in the past. According to Attribution theory, if an organization is constantly experiencing similar crises, it means that it lacks control and there is an ongoing problem that has to be resolved (Martinko, Douglas, Ford & Gundlach 2004).

Lastly, the third component -prior relational reputation- pertains to the reputation an organization has, based on its behavior to its stakeholders in another context (Porritt, 2005). If stakeholders believe that they have not been served efficiently in the past, prior relational reputation is a defect. On the contrary, it can operate as an asset if stakeholders are of the opinion that they have received their services in a favorable way (Porritt, 2005). A negative prior relational reputation suggests that the organization demonstrates little consideration for stakeholders in general, and not only in the case of a crisis.

After examining the elements that shape a crisis, the SCCT model focuses on the behavioral intentions of individuals, which includes purchase intention and negative word of mouth. However, negative word of mouth is considered sometimes as defective and difficult to measure (Coombs & Holladay 2010). In fact, people tend to forget about specific incidents that were considered as crises in the past. Therefore, a post online may remain for years, but people's memory about the incident will fade as time passes.

Moreover, the SCCT model holds that the way an organization communicates during a crisis affects people's perception of the incident. It provides a sum of crisis response strategies which can be used to repair the reputation, reduce the negative results of an incident and prevent undesirable behaviors (Coombs, 2007). Therefore, three types of initial response strategies are identified: (1)denial: stipulate that no crisis exists, (2)diminish: alter the attributions about the crisis event to make it appear less negative to stakeholders, or (3)rebuild: generate new reputational assets (Coombs, 2007). In the denial strategy, organizations dissociate themselves from the crisis. Managers note that there is no crisis, and if this is the case, then there is no reputational damage for the organization. However, in case that there are rumors, managers should communicate that there is no "real damage" and provide evidence about their claim. Consequently, if the media and the stakeholders accept this claim, there will be no reputational damage. Diminish strategy is used by managers to support that a crisis is not as bad as individuals may think, or they couldn't control the crisis. In this case, if stakeholders believe the organization, there will be no severe reputational lost. On the contrary, if stakeholders reject the claim of the organization, then they will be exposed to an array of information which means that it will be up to them to choose which information they find more credible to keep themselves updated regarding the incident. Furthermore, rebuilding strategies are mostly used when a crisis poses severe threats to the reputation of an organization. This strategy attempts to improve the reputation of a corporation by providing to stakeholders and victims symbolic aid of how to confront the crisis. Last but not least, bolstering is mentioned as another crisis response strategy but a secondary one. This strategy is used to remind stakeholders about the good performance of the

organization in the past, or emphasize that the organization is a victim of the crisis as well (Coombs, 2007).

SCCT argues that every crisis response should begin with instructing and adjusting information. Regarding the former, instructing information notify stakeholders on how to protect themselves in the case of a crisis. For instance, information includes a guide on how to evacuate an area during an incident or what steps to take in order to protect their data from a cybersecurity incident. Adjusting information assists individuals to handle a crisis from a psychological perspective. For instance, expression of questions, emotions or information regarding the crisis incident can be considered as adjusting information (Coombs, 2007; Coombs & Holladay, 2010).

The final component of SCCT model is the matching process between the type of crises mentioned and the response strategies. The first cluster (victim cluster) which have a low rate of attributed responsibility, can be handled through the usage of both instructing and adjusting information (Coombs & Holladay, 2010). Therefore, when an organization is also considered as a victim by the stakeholders, both tactics are effective in order to manage the crisis. Secondly, in case of a crisis which is seen as an intentional action, the response of the organization should include instructing and adjusting information, but also accompanied with an apology and/or compensation (Coombs, 2007). Lastly, in the case that a crisis is considered as accidental, the diminish strategy should be followed in order to remind stakeholders that the situation could not be entirely controlled by the organization.

To conclude, it is important to adopt the SCCT model as, it foresees the reaction of people to the crisis response strategies implemented by the organization to regulate the crisis (Coombs, 2007). Hence, an evidence-based crisis communication guideline is needed in order to implement the right steps so as to identify the crisis type and assess the reputational threat. However, since the topic of the research refers to the results of the crisis on the reputation of the organization as well as on the type of online behavior of Facebook users, another model is also needed. In fact, the SCCT model examines only two types of stakeholders' behaviors: the possibility for the consumer to end the relationship with the organization and/or negative WOM.

## 2.2. Social Mediated Crisis Communication model

The second theoretical model that will be used, is the Social Mediated Crisis Communication (SMCC) model. In contrast with the SCCT model, SMCC theory does not only take into account the crises type and the responsive strategies but also tries to include the existence of social media within this context. What's more, SCCT model examines the post-crisis reputation of the organization as well as the negative word of mouth as outcomes by the crisis communication strategies, while SMCC theory is trying to incorporate the form and source of information (traditional media, social media, offline word of mouth communication) as a determiner which can impact the public's behaviors during and after a crisis (Austin, Fisher & Jin, 2012).

Over the past two decades, social media has evolved to an increasingly omnipresent means of interaction, information, and expression of identity (Ashley & Tuten, 2015). Before expanding upon the model which incorporates social media in the context of crisis communications, this study presents two well-known definitions of social media. Firstly, according to Fraustino, Liu and Jin (2012), social media are "interactive digital tools that feature content users may generate, manipulate, or influence" (p. 7). Additionally, Wright and Hinson (2009) emphasized more on the role of social media from the perspective of public relations and described social media as digital tools which facilitate the interaction and the exchange of content between individuals and organizations. More specifically, these are the platforms where the communication between organization and stakeholders, as well as amongst the public is interactive and includes a two – way conversation (Wright & Hinson, 2009).

The rise of social media has altered the background of crisis communications in at least two essential ways. Firstly, social media platforms constitute the source or origin of an organizational crisis, such as a mishandled or not well-designed campaign or a message that can have a negative impact on a corporation's reputation (Austin & Jin, 2016). Secondly, these digital platforms have the power to promptly transmit a rumor, negative emotions and opinions in relation to an organization (Austin & Jin, 2016). Hence, an instrumental advancement in crisis communication research has emerged, and this was the shift from the sender orientation to a receiver orientation (Coombs &

Holladay, 2014). During crises, social media constitute new platforms where online word of mouth is performed, operating as a formal and informal communication channel in which opinions and organization information are conveyed, shared and processed (Austin, Fisher & Jin, 2012).

When crises emerge, individuals' behavior on social media can change dramatically, which makes crises even more unpredictable and hard to control. According to a recent research (Pew Internet & American Life, 2006), during crises, the usage of social media by the public increases to a high degree and this phenomenon has a direct and indirect impact on stakeholders (Lariscy, Avery, Sweetser, & Howes, 2009). On the one hand, a rise in social media usage can lead to a great propagation of a crisis, which sometimes leads to dramatic turns. However, this augmentation of use can be proved fruitful for the organizations as well, as they are able to respond immediately to the incident and have an interactive and effective communication with their stakeholders (Austin, Fisher & Jin, 2012).

Within the context of social media as an environment where crises also take place, an essential aspect that influences the public's perceptions about an incident is individual's choice of channel for their update or propagation of their own feelings and opinions. Their selection of the channel of communication during a crisis is based on four themes which are: humor/entertainment value, the ability to share insider information, social norms and privacy concerns (Austin & Jin, 2016). To be more specific, certain social media channels such as Facebook, Twitter and blogs, are the primary platforms in which the public gather and share information about an incident, especially in the first 12 hours of a crisis, when the highest amount of user-generated content is created online (Heverin & Zach, 2010; Wigley & Fontenot, 2010). Interestingly, a study found that when individuals receive information regarding a crisis from Twitter they are less likely to blame the organization (Schultz, Utz & Goritz, 2011). Another element that can influence the public's behavior and involvement during a crisis is Electronic Word of Mouth (eWOM) (Kozinets, de Valck, Wojnicki & Wilner, 2010). However, the public is involved to eWOM and spreads information regarding an incident, only when they judge that it is appropriate and the information will be valuable to potential recipients (Sohn,

2009). Further, when individuals feel betrayed and dissatisfied, they may use social media in order to spread negative opinions and feelings on and offline (Bailey, 2004; Richins, 1983). This negative WOM can take the form of a revenge towards the organizations or an effort to convince others to act against an organization (Ward & Ostrom, 2006).

Previous literature has discussed the different motives behind the usage of social media during crises. To begin with, Johnson & Kaye (2010) highlighted that people seek out social media because they provide an up-to-date mean of communication. In addition, Choi & Lin (2009) claim that people choose social media as a mean of emotional support and sharing of information or emotions. Lastly, another opinion is that individuals go online during crises to find information that they could not find on traditional media (Bucker, 2002). The Blog Mediated Crisis Communications model, which was the initial version of the SMCC model, proposed that the public goes online and uses blogs for the following three motivations: to find information about the current crisis, to share information that is not available from other means of communication such as news media; and thirdly to share its experience (positive or negative) regarding the crisis or the organization with others, which creates a sense of compassion and excitement (Jin & Liu, 2010). Taken into account all these motivations that drive people to use social media, the social media messages, posted by people interested or affected by a crisis, are crucial to the organization's reputation. On the one hand, these messages can determine the post-reputation of an organization, while on the other hand, they afford researchers the opportunity to examine whether certain crises responses have the desired effects, such as maintaining purchasing intentions (Coombs & Holladay, 2014).

In order to understand the role of social media use by the public in crisis communication, four key areas have to be investigated according to Austin and Jin (2016). The first key area is the social media engagement an organization has before, during and after a crisis (organizational approach and considerations). The second area refers to the audience-oriented approaches and considerations. In this case, the investigation of the audience's characteristics of an organization, such as their behavior when they seek, produce and share information, before, during and after a crisis. These

characteristics, in combination with the public's motivation, can influence their behavior on social media when an incident occurs. The third key area presented by the authors refers to the characteristics of the crisis, which can also play an instrumental role in people's use of social media (Austin and Jin, 2016). Last but not least, the special characteristics that each social media platform has can affect the nature of crisis communication and the usage of social media by the public. Hence, certain types of social media, such as Twitter or Facebook can have different effects on people's perception about a crisis and therefore these platforms provide outstanding opportunities for organizations to address and utilize in their crisis communication strategy. More specifically, the reason these platforms provide different opportunities for organizations lies upon the unique design of each social media platform. For instance, while Twitter is designed to enable users to share only short text messages, other platforms such as Facebook, email, and blogs give the public and the organizations the opportunity not only to upload a short text but also accompanying it with multimedia files (Mills, 2012). Grounded on this fact, it is reasonable to believe that the plethora of information a message has, as well as its extent and its diversity in content (e.g. combination of texts and videos) can have a different effect on public's perception, as individuals are exposed to different sources and different forms of information.

As mentioned earlier, the SMCC model is originated by the Blog-Mediated Crisis Communication (BMCC) model (Jin & Liu, 2010). The latter was created in order to give an insight on how to identify influential blogs and create the right communication strategy for the specific blogs, before, during and after an incident. According to the authors of this theory, influential blogs satisfy the need for information and supporting of users' emotions, by providing timely and accurate facts on matters that interest and affect personally the blog followers. Therefore, a checklist matrix was created to assess the influence of blogs and simultaneously give recommendations about the appropriate responses and communications strategies based on the characteristics of the blogs. However, this model has evolved into a model which now includes all types of social media and not only blogs and thus, was renamed to the Social Mediated Crisis Communication (SMCC) model (Austin, Liu & Jin 2012).

The SMCC model illustrates and explains the relation between the following key concepts: the organization, social media, traditional media, offline WOM, and key public, before, during and after a crisis (see Figure 2). Regarding the latter, the authors of the model segmented the public into three different categories based on their behavior online. Therefore, individuals who produce and post information about a crisis are named influential social media creators, while people who consume this kind of information and share it on their online and offline environment are called social media followers. Lastly, the third category is related to the public which doesn't participate actively on social media but still consumes information about the crisis either through traditional channels or through social media followers and other inactives (Austin & Jin, 2016).

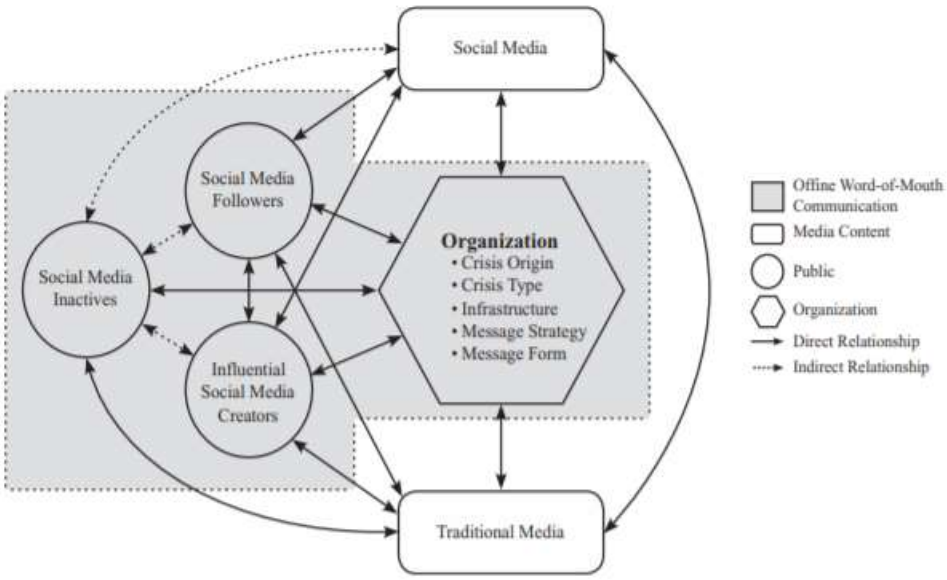


***Figure 2.2.*** *Social Mediated Crisis Communication Model (Austin & Jin, 2016)*

The SMCC model has further explored the impact of the form and the source on information seeking and sharing during a crisis. Findings revealed that when an incident occurs, individuals seek primarily information on traditional media rather than social media, due to the fact that they find them more accurate and credible. Their choice of information, however, affects their behavior and perception about the organization. For instance, when people receive information from traditional media, they are more likely to talk more positively about the organization. Similarly, when a crisis is communicated through social media, the public tends to share and post positive comments about the

organization (Austin & Jin, 2016). On the contrary, individuals were most likely to communicate in a negative way about an organization when they initially receive information about a crisis through the corporation's offline word-of-mouth communication (Austin & Jin, 2016). Last but not least, just like the SCCT model, the SMCC model also examines the emotions experienced by the public based on the form and source of information. Previous research has proved that when the public receives information about a crisis of internal origin by a third party through social media, it is more likely to feel anger, disgust, and contempt (Austin & Jin, 2016).

To conclude, the authors of the SMCC model have encouraged researchers to use this model to further explore how a specific type of crisis can affect the behavior of the public on social media (Austin & Jin, 2016). Consequently, this model is significant for this research, as its purpose is to examine whether certain variables such as crisis responsibility, CEO's credibility, and pre-crisis reputation have an impact on the users' online behavior (Secondary Crisis Communications) after a cybersecurity attack. In this study, Secondary Crisis Communications differs from the traditional meaning of the term. In fact, here Secondary Crisis Communications is not focused on the traditional approach of the term which is the face – to – face interaction between the spokesperson of the organization and individuals who had experienced a crisis, in which someone can draw upon an array of signals within a social context (Knapp & Daly, 2002). Since this study is trying to have a more complex approach to crisis communication and incorporate the interaction between users on social media, secondary crisis communications in this case concerns the engagement of the public with social media directly after a corporate crisis and is perceived as the willingness of stakeholders to talk about a crisis and propagate the information of a crisis through commenting, sharing or informing (Bi, Zheng & Liu, 2014).

### 2.3. CEO's credibility

As mentioned in the introduction, an aspect that will be taken into account regarding its impact on post-crisis reputation and secondary crisis communications is the credibility inspired by the CEO. Chief Executive Officers (CEO) are closely associated with the organization's vision, strategic planning, policies, corporate communications and culture

(Flatt, Boundy & Wagner, 2013; Treadway, Adams, Ranft & Ferris, 2009; Fombrun, Ponzi & Newburry, 2015). These elements are in fact, the same variables that drive enterprises' reputation, and thus, the role of the CEOs in organizations is of utmost importance as they are the ones who are highly visible to both external and internal stakeholders (Flatt et al., 2013). Additionally, as Fombrun and van Riel (2004) claim "a favorable impression of a CEO enables people to put a face on the faceless and create meaning out of uncertainty" (p.235). Previous findings have validated the aforementioned argumentations. For instance, in 2012, a survey regarding the relationship between the CEO and the reputation of a company was conducted on consumers and senior executives in developed markets ( the United States and the United Kingdom) and emerging markets (China and Brazil) (Weber Shandwick and KRC Research, 2012). In the results, it was indicated that senior executives accredited nearly 49% of their organization's reputation to the reputation of the CEO. Additionally, 66% of consumers noted that their opinion and perception on the CEO of a company influence their view on the reputation of the company. Moreover, another research mentioned a survey conducted in 2003 in which it was revealed that respondents indicated that at least half of the reputation of an organization is based and attributed to the reputation of the CEO (Turk, Jin, Stewart, Kim & Hipple, 2012). Last but not least, there is extensive research on how changes in the position of a CEO can have a positive or negative impact in the market, the performance of a company and the behavior of stakeholders grounded on whether the CEO is considered as an outsider or insider for this position.

Interestingly, several scholars argue that CEOs nowadays are not only viewed as representatives of organizations, but also as distinct personal brands, or even as celebrities (Chen & Chun, 2017; Sinha, Inkson & Barker, 2012; Treadway et al., 2009). In fact, a significant percentage of CEOs have such a high reputation that exceeds the reputation of the company (Flatt et al., 2013; Turk et al., 2012). Based on previous research, the CEO's celebrity is a social structured element (Sihna et al., 2012). This means that the expectations, as well as the consequences of CEOs' actions, are mostly constructed by opinions and interpretation of the public (Hayward et al., 2004; Khurana, 2002). Therefore, the role of the media is highly essential, as it determines the framework

within which individuals create meaning and form opinions (Sinha et al., 2012). If the media portrays the actions of a CEO as a decisive driver to the company's success, the CEO can take delight in his/her fame and leverage this recognition in order to create a strong impression of future success in the market and most essentially establish a strong feeling of trust and commitment amongst its stakeholders (Fombrun et al., 2005; Sihna et al., 2012). Consequently, the real strength of a celebrity CEO relies on the involvement of intermediaries and other stakeholders (Treadway et al., 2009). This is the reason why in this research, it is argued that attitudes towards CEO correspond to a "context of credibility" (Treadway, Adams, Ranft & Ferris, 2009). However, the ability to transform this social capital into a long term reputation and relationship with the stakeholders does not apply to all CEOs, and thus this is a unique skill that a small percentage of CEOs possess (Ketchen, Adams, & Shook, 2008).

Taken all the aforementioned into account, CEOs' reputation and credibility is essential in the case of a crisis (Seeger & Ulmer, 2001). The CEO is oftentimes appointed as the representative or the spokesperson of the company and his or her presence aspires authority (Seeger & Ulmer, 2001). Simultaneously the CEO may also decide on the moral tone for the crisis response (Seeger & Ulmer, 2001). Prior attitudes towards a CEO of an organization can be closely associated with the image of the corporation and affect the public's opinions during a crisis. Since CEOs aspire credibility (Alghawi, Yan & Wei, 2014) and are oftentimes regarded as spokespersons who shape future expectations they have the power to direct and influence people's perceptions about the crises or even inspire a sense of control, since they are mainly responsible for all outcomes (Treadway et al., 2009; Chen & Chun, 2007). Thus, a favorable reputation towards a CEO can operate as a halo or capital. When a crisis occurs, CEOs take advantage of this capital by directing the public's opinion in order to achieve the desired outcome which in this case is the circumvention of a reputational loss or damage (Fombrun et al., 2015; Gainess & Ross, 2002; Westphal & Deephouse, 2011).

In this research, it is assumed that organizations who have CEO's regarded as celebrities or highly credible will not suffer from a great reputational loss. In fact, if the public trusts and admires the CEO of the organization, their perception regarding a crisis

might be driven by its feelings about him or her. Hence, it will be more possible for the CEO to direct their behaviors and their perceptions concerning the incident towards a more positive path, which will ultimately lead to lower reputation damage. Consequently, it is expected that since the CEO can drive and control the behavior of the stakeholders who attribute great credibility to him, users will be less likely to 'spread' the message of the crisis on social media or comment negatively about the organization. Based on this assumption, the following can be claimed:

*H1a: CEO's credibility has a positive impact on the post-crisis reputation of a firm in the case of data leaks in a cybersecurity crisis.*

*H1b: CEO's credibility has a negative impact on secondary crisis communication in the case of data leaks in a cybersecurity crisis.*

### 2.4. Pre-crisis reputation

Reputation can be translated as the assessment which stakeholders make concerning an organization (Coombs & Holladay, 2006). It is proved that a favorable reputation towards an organization can lead to significant results such as attracting customers and exceptional employees, increasing job satisfaction, creating interest for investments, raising the motivation of the employees as well as producing positive media coverage (Alsop, 2004; Roberts & Dowling, 2002; Fombrun and van Riel, 2003). As aforementioned in chapter 2.1, pre-crisis reputation is one of the most important characteristics in order to evaluate the risk of a crisis in a corporation, and is considered more important than other elements such as the crisis history of the organization (Coombs, 2007; Coombs & Holladay, 2006; Sheldon & Sallot, 2009). As Fombrun and van Riel, (2003) claim, reputation is built upon relationships between stakeholders and organizations and thus operates as a "capital" that every organization possesses.

Previous research has indicated that before a crisis occurs, favorable prior reputation can serve as "reputational capital" (Coombs & Holladay, 2006). Reputational capital can be defined as "stock of perceptual assets and social assets" (Fombrun & van Riel, 2004, p. 32). Thus, just like banks pay attention to increasing their capital in order to be ready for possible threats, organizations should also focus on building this

reputational capital. When an incident occurs, the organization starts losing some of its capital. However, if prior reputation is high, organizations can spend more of their capital than organizations with unfavorable or neutral reputation. Consequently, if this capital is high, stakeholders might not react negatively and therefore the reputation of the organization is not affected significantly. In fact, companies with high reputational capital may remain strong and not affected by the crisis (Coombs, 2007).

Another similar theory is depicting prior reputation as a halo or shield (Coombs & Holladay, 2006). Caponigro (2000) claims that a good prior reputation might influence the stakeholders' evaluation of an organization, in a sense that they might give the organization the "benefit of the doubt" and contribute less responsibility for the crisis. This argumentation is based on a psychological theoretical framework known as expectancy confirmation (Coombs & Holladay, 2006). Expectancy confirmation theory examines individuals' perceptions about social issues and was articulated by Edwards and Smith (1996). Grounded in this theory, cognitive dissonance play a significant role in people's opinions during a crisis, as individuals try to acquire information that resembles their previous beliefs of an issue. Hence, when a crisis occurs, every adverse information is interpreted in a way that is aligned with the individuals' prior beliefs (Coombs & Holladay, 2006). Additionally, there is a possibility that these people will also ignore negative comments and information about the crisis and will tend to focus only on the positive aspects of the organization (Coombs & Holladay, 2006). Simultaneously, the media and other stakeholders will persist in supporting the organization, rather than criticizing. As a result, the more people are involved and engaged with an organization, the less the possibility is to change their attitudes and perceptions about the company and therefore, the threats of a crisis are less likely to provoke reputational damage (Coombs & Holladay, 2006). Nevertheless, it is essential to mention that the theory of the halo effect has not been tested in the context of cybersecurity crises. Empirical evidence exists in the case of other types of crises which led Coombs and Holladay (2006) to claim that a favorable pre-crisis reputation can operate as a halo effect or as a shield, but only in the case of organizations with very favorable prior reputations. Thus far, research has shown that an unfavorable reputation can influence people's behavior when attributing

responsibility during a crisis, but this doesn't prove that a favorable pre-crisis reputation can operate as a shield. In fact, studies measuring the effect of prior reputation to the post-crisis reputation of organizations have indicated that favorable and neutral reputation didn't differ from one another (Klein and Dawar, 2004; Coombs and Holladay, 2002). Only unfavorable reputation was indicated to produce greater blame attributions to the organization during a crisis (Klein and Dawar, 2004; Coombs and Holladay, 2002). Nevertheless,

Other scholars who have examined the effect of prior reputation to the post-crisis reputation of an organization found that a good prior reputation can positively influence individual's opinions and behaviors towards the organization (Carrol, 2009). Respectively, Kiambi and Shafer (2015), discovered that a good prior reputation resulted in a higher post-crisis reputation as well as a lower possibility for negative word of mouth. Similarly, Lyon and Cameron (2004) discovered that there were more positive attitudes towards organizations with a good established prior reputation than companies with a medium or bad prior reputation. Nevertheless, the majority of the existing research is based on assumptions and opinions rather than empirical research (Dowling, 2001). Hence, more empirical evidence is needed in order to prove whether pre-crisis reputation plays a pivotal role on the protection of the organization's reputation after the crisis (Coombs, 2007; Kiambi & Shafer, 2015).

On the other side of the spectrum, there is a significant percentage of scholars who claim that a prior favorable reputation might sometimes be a liability (Dean, 2004; Rhee, & Haunschild, 2006; Grunwald & Hempelmann, 2010). They argue that a high reputation creates greater expectations concerning the product provided by the organization and they entitle this psychological phenomenon as "expectancy violation effect". Based on this theory, people react more aggressively and strongly to events that infringe their previous expectations of how the organization should behave and hence a prior high reputation can operate as "boomerang" for organizations (Dean, 2004; Rhee, & Haunschild, 2006; Grunwald & Hempelmann, 2011). However, while these empirical pessimistic findings also exist, the optimistic view is leading (Sohn and Lariscy, 2015).

Given such an ongoing debate, in this research, it is assumed that in the case of data leaks, a favorable reputation is expected to positively influence people's perceptions regarding the crisis. Individuals may be more willing to give the organization the "benefit of the doubt" especially if it is the first time that they experience such an incident and may pay more attention on how they can overcome this crisis, rather than stop their relationship with the organization. Therefore, it is presumed that this kind of behavior will result in less engagement of users with social media and less willingness to propagate the message of the crisis. Consequently, the following hypotheses are proposed:

*H2a: A high pre-crisis reputation is likely to have a positive impact on the post reputation of the organization in a cybersecurity crisis.*

*H2b: A high pre-crisis reputation is likely to generate less secondary crisis communication in a cybersecurity crisis.*

### 2.5. Crisis Responsibility

Crisis responsibility refers to the amount of the attributed blame to an organization, by the stakeholders when a crisis occurs (Coombs, 2004). The attributed responsibility can be either due to internal or external factors which in turn impact peoples' behavior towards the main actors of the crisis (Coombs, 2010). However, in the case of internal responsibility, research has shown that negative behavioral reaction can be detected (Weiner, 2010). On the other side of the spectrum, if the crisis is considered as a result of external factors and the level of the attributed responsibility is high, then behavioral reactions are positive (Weiner, 2010). Overall, it can be claimed that the blaming process during a crisis is based on the stakeholders' opinion about the incident and whether they consider the incident intentional or a result of an unforeseeable event (Jin, 2010).

Moreover, as mentioned in the SCCT model, the level of the attributed responsibility to an organization can create emotions such as anger or sympathy. According to the literature, these emotions are significantly correlated with the level of responsibility (Choi & Lin, 2009b). Hence, the higher the level of responsibility, the more likely it is for people to feel anger. On the contrary, when the degree of

responsibility is low, people are more likely to feel sympathy towards the organization. Consequently, when the level of responsibility is significantly high, the organizations are threatened by a great reputational risk (Coombs, 2007). Lastly, grounded in previous research, crisis responsibility does not only affect peoples' emotions but also purchasing behaviors, negative WOM and even the possibility for the consumer to end the relationship with the organization (Coombs, 2007).

Based on the results of former findings, the level of crisis responsibility has an effect on the reputation of an organization after a crisis. In this research, it is speculated that a cybersecurity crisis and especially data breaches can be attributed most of the times to intentional purposes as organizations owe to follow certain regulations and be transparent regarding the privacy settings of their platforms. What is more, a data breach harvests personal data that can have detrimental impacts on users personal and professional life. Thus, the attributed blame by the stakeholders will be significantly high and thus, lead to a great damage reputation. Simultaneously, as high responsibility is attributed to organizations who have experienced cyber cybersecuritys, individuals will be more willing to share their experience and spread the message of crisis on social media. Consequently, the following hypotheses are posed:

*H3a: The higher the attributed responsibility to a company, the higher the damage to the reputation of the company in a cybersecurity crisis will be.*

*H3b: The higher the attributed responsibility to a company, the higher the levels of secondary crisis communications in a cybersecurity crisis will be.*

### 2.6. Conceptual model

To recapitulate, in this study, six hypotheses were formulated, founded on previous literature and empirical findings. Figure three depicts the conceptual model of this research, which provides a visualization of the overview of all hypotheses.

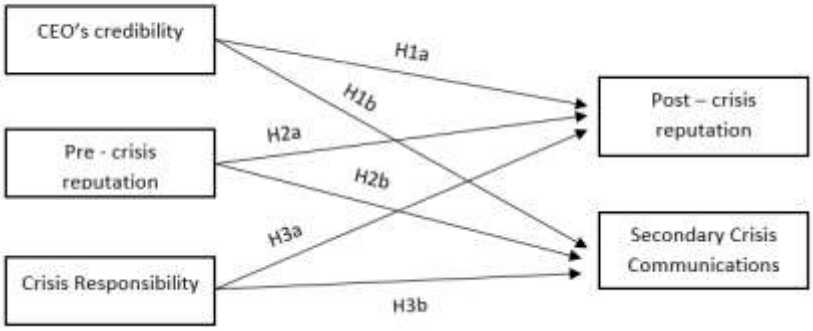


*Figure 3 Conceptual model of the research*

## 3. Methodology

This chapter will present and explain the method that was used in order to examine the above stated conceptual model. Hence, it describes elaboratively the syllogism for the choices made in relation to the research design, data collection, sampling method as well as the operationalization of the theoretical concepts.

### 3.1. Choice of Method

In order to effectively answer the research question underlying this study, the quantitative methodology was considered as the most appropriate. According to Babbie (2011), quantitative research methods are based on several assumptions or expectation that a researcher has, based on previous theory. Thus, it often uses a deductive approach and when these variables are finally tested, a researcher can discover whether they actually happen or not (Babbie, 2011).

Besides testing the hypotheses imposed, quantitative research methods facilitate the analysis of the relationship between dependent (post-crisis reputation and secondary crisis communications) and independent variables (crisis responsibility, CEO's role as a message source and pre-crisis relationship) (Punch, 2014). What's more, these research methods allow not only generalizations but also forecasting certain matters (Zhou & Sloan, 2011). As the main goal of the present study is to test relationships between theoretical concepts, a quantitative methodology was considered as the most suitable option. More precisely, a quantitative online survey will be conducted. As Punch (2014) points out, a survey is used to emphasize the analysis of relationships between different variables. The survey was created in Qualtrics and disseminated to different Facebook groups which were found based on keywords such as 'social media', 'technology', 'cyber security' and 'data leaks'. Some of the groups that the researcher posted the link to the survey are the following: 'Social Media New Network', 'Latest Technology News and Updates', 'EU GDPR (General Data Protection Regulation) & E-Privacy Regulation' and 'Cyber Security and Hacking (CSH)'.

One aim of quantitative surveys is to comprehend people's opinions and values that are relevant to the research (Neuman, 2014). Furthermore, a survey is often used to

ask for the behavior, attitudes, expectations, and characteristics of people and it allows the self-classification of the participants (Neuman, 2014). As explained in the introduction, this research is interested in individuals' perspectives about a specific incident of data leaks and how these opinions may have an impact on their use of social media platforms and the reputation of the organization after a cybersecurity incident. These are all latent variables. As Salkind (2010) highlights, latent variables are considered as variables that cannot be observed. Nevertheless, their presence might be noticed by their consequences on variables that are observable (Wagner et al., 2012). In order to examine these latent variables, researchers have created scales, each of which measures a certain type of behavior, where participants are enabled to evaluate attitude statements from "strongly agree" through "strongly disagree" (Matthews & Ross, 2010).

An online survey has clear advantages, which can be proved effective for the relevant study. First of all, the method can reach a wide range of the population and derive data within a very short period of time (Rice, Winter, Doherty and Milner, 2017). In fact, as the majority of the population has access to the Internet, the issue of lacking representatives cease to exist (Evans & Mathur, 2005). Furthermore, it is a flexible tool as they can be conducted in several formats and tailored according to users' demographics, language, and location (Evans & Mathur, 2005). At the same time, it also allocates anonymity for the participants, thus people may feel more comfortable to answer truthfully to matters that may are sensible (Rice et al., 2017). In addition to that, this method is cost effective, but most importantly, it gives the researcher the opportunity to generalize the findings from the sample to a larger population (Rice et al., 2017)

On the other side of the spectrum, the method also has several drawbacks that need to be addressed. The most important defect is the self-selection of the respondents, which oftentimes leads to a low response rate (Möhring & Schlütz, 2010). In fact, it is up to the participants to decide whether they want to participate in the survey or not (Rice et al., 2017). This issue may have a negative effect on drawing a random and representative sample (Punch, 2014). Nevertheless, due to the majority of the benefits, the application of this method is presumed suitable and the questions that will be asked in order to measure the dependent and independent variables are presented on Appendix A.

Lastly, the choice for this specific methodology can also be justified by the lack of quantitative survey methods in crisis communication research. Despite the fact that research in the field of crisis communication has increased rapidly (Kim & Cameron, 2011), the methods that were used in order to derive meaningful insights have focused on case studies and experiments (Kiambi & Shafer, 2015). Although case studies provide valuable descriptive data (Coombs & Holladay, 2008), they oftentimes offer little theoretical understanding of crisis communication (Dean, 2004) and are hard to generalize (Carroll, 2009). Additionally, experiments are based on constructed and/or fictitious crises and organizations (Lyon & Cameron, 2004), which urges the need for quantitative research in relation to real events and organizations (Dean, 2004). This need was also highlighted by Johnson Avery, Weaver Lariscy, Kim and Hocke (2010) in a literature review in the field of crisis communications. The aforementioned scientists noted that the use of surveys would add value to this scientific field by broadening and diversifying the methodological approaches that have already been used to derive outcomes. Hence, the present study incorporates this suggestion, and applies a quantitative survey that investigates the real crisis of Facebook – Cambridge Analytica.

### 3.2. Sampling Method

This research's target population consists of all Facebook users. Based on a recent research, Facebook is comprised of 2.27 billion users as of the third quarter of 2018, making it one of the top social media networks (Statista, 2019a). Taken this into account, reaching all users was an impossible task, thus the goal was to reach 150 to 250 participants.

In order to reach the amount of desired respondents, the convenience sampling was applied. This sampling method constitutes one of the most well-known non-probability sampling methods (Sarstedt, Bengart, Shaltoni & Lehmann, 2018). The sampling is based on the easy accessibility of the respondents by the researcher. In fact, as mentioned before, Facebook users represent a great percentage of the entire population, therefore, it will be impossible to reach all of them. Convenience sampling, allows the researcher to find possible respondents in a short period of time, as their

participation depends on their willingness to be part of the research and at the same time it is proved that it is cost efficient (Walliman, 2006; Etikan, Musa, Alkassim, 2015).

Despite the fact that non-probability sampling has been applied several times in academic research due to its convenience benefits (Etikan, 2016), it is claimed that results derived from this kind of sampling method can be biased (Sarstedt et al., 2018). The main argument which supports this claim is that the members of the selected population are homogeneous (Etikan, 2016). Initially, the link of the survey was posted on the researcher's university Facebook page as well as to her own profile. However, in order to prevent collecting data from a homogeneous population, the link to the survey was also shared on different Facebook groups. To be more specific, the researcher searched on Facebook different Facebook groups using a variety of key terms that were relevant to the research such as "data leak", "social media", "technology" and "data security". Some examples of the groups found are the following: "Social Media News Network", "Social Media and Bloggers Community" and "EU GDPR (General Data Protection Regulation) & E-Privacy Regulation". After joining these groups, the link of the survey was posted and was accompanied with a short text requesting from the participants to participate in this research for the purpose of an academic thesis project and forward this link to their peers. This approach aimed at reaching a significant percentage of the population that was beyond the researcher's personal network and could be as heterogeneous as possible in order to be considered representative and accurate for the conduct of the research.

## 4. Data Analysis

In this subsection, the analysis of the data which was derived by the digital survey will be discussed. The tool that was used in order to implement the analysis was the IBM SPSS Statistics 24.

### 4.1. Pre-Test, Data Cleaning

To begin with, the online survey of this research was created on Qualtrics. Before proceeding with the collection of the data for the research, the quality of the questions, as well as their clarity and structure, were tested in a pre-test. In fact, 15 participants received a link to the survey and after filling it out, they were asked to give their opinion on the comprehension of the questions as well as their suggestions for improvement. The feedback of the respondent was vital for the final form of the survey, as some questions were removed from the questionnaire, while others were altered in order to be more clear to the respondents. A representative example is a statement that respondents had to evaluate on a seven-point Likert scale that was measuring the secondary crisis communications. More specifically, in this variable, there was an item which asked the participants "how likely they are to leave a reaction against Facebook on social media" after they found out about the Facebook – Cambridge Analytica scandal. Since the majority of the respondents couldn't understand what "leaving a reaction" actually means, the questions were altered to "how likely are you to comment against Facebook on social media?". Another similar adjustment was also made to an item in the same variable. More specifically, the first item of the scale was asking from the participants to answer on a seven-point Likert scale how likely they are "to share the message with other people". Again, the question was not clear to the majority of the participants in the pre-test and thus, a clarification was made in this question that was mentioning that "share the message" can mean forward, show or retweet the message of a crisis on social media. The final design of the survey, as well as its questions, can be found in Appendix A.

The data collection took place between 24 April and 2 May 2019. During this period, a total of 158 people responded to the survey. However, while cleaning the data it was noticed that 3 respondents spent less than one and a half minute to respond to the questionnaire and thus, they were removed from the sample, as it was assumed that they

did not spend the necessary time to process the questions and answer appropriately. This resulted in the final size of the sample which was comprised of 155 people.

Moreover, as part of the data cleaning process, some questions that were reverse-coded were recorded in order to prevent response bias (Pallant, 2007). Simultaneously, this action enabled an easier way to use and analyze the data, as well as interpret it. A representative question that was formed in a negative way and had to be reversed was the following: "I do not trust Facebook to tell the truth about the emissions scandal". Finally, open answers regarding the age and the nationality of the participants were examined and checked for any errors. In the case of the nationality of the participants, some adjustments were made as the SPSS couldn't categorize the same nationality with a different wording into one group. For instance, people who wrote "Greek", "Greece" and "Hellenic" as their nationality were enlisted in different categories, although both people have the same nationality. Therefore, the researcher had to check the answers of the respondents and classify them again into new categories, in order for the data to be reliable.

### 4.2. Operationalization and Measurements

In this subsection, the operationalization of the theoretical concepts will be discussed as well as the scales that were used in order to measure the variables included in the research. In the case of surveys, operationalization refers to the modification of the research question into specific questions that can be asked to the participants in order to test the independent and dependent variables of the research and derive significant data (Möhring & Schlütz, 2010). In this study, all the measurements that were used, were based and implemented on previous studies in the field of crisis communication. In addition, since the questionnaire refers to every nationality, it was written and formulated in the English language, in order to be comprehensive for all of the participants. Last but not least, all questions were adjusted to the Facebook – Cambridge Analytica scandal, meaning that the questions were formulated and always referred to the scandal or the CEO of Facebook, Mark Zuckerberg in order to be more intelligible by the audience.

For the coherent and logical structure of this research, the operationalization for each variable will be presented separately, so readers can have a clear idea of all steps

taken for each variable separately and in one section. Before testing the hypotheses imposed in the research, the reliability of the measures as well as the correlation of the items within each scale had to be tested (Pallant, 2007). The first step of the process concerns the reliability test of the measurements that were used based on the literature. Despite the fact that all the scales derived from the literature had a high value of Cronbach's a, the aim of this step was to validate that the Cronbach's alpha of each scale was adequate for this research in particular. The second step that was followed for both independent and dependent variables was the conduct of a factor analysis. Factor analysis is a statistical data reduction and analysis technique. Its usage doesn't aim at testing hypotheses or correlation among different variables. On the contrary, factor analysis is designed to develop and evaluate the items included in a scale that was used to measure a variable (Pallant, 2007). To be more specific, the scale developer begins with a great number of items and questions that were used to measure a variable and, through the usage of this analytical tool, researchers are able to reduce these items in order to create a shorter, but always coherent subscale (Pallant, 2007). Therefore, it indicates whether the questions that were included in the questionnaire to measure each variable, belong to one factor or there are multiple factors within one scale that measure different dimensions and thus, have to be separated. Since there are two types of factor analysis based on the literature, it is vital to mention that in this case, the exploratory factor analysis was used, since the aim of the analysis was to find correlations within a set of variables. Lastly, for the exploratory factor analysis of all variables in this study, the usage of the maximum likelihood factoring with a Varimax rotation was deployed. The factor analysis and the factor loading for every variable can be found at Table 4.1.

***Table 4.1.*** *Factor analyses and reliability analyses of scales measuring Crisis Responsibility, CEO credibility, Pre-Crisis Reputation, Post-crisis Reputation and Secondary Crisis Comunications*

| Item | Crisis Responsibility | CEO credibility | Pre-crisis reputation | Post-crisis Reputation | Secondary Crisis Communications |
|---|---|---|---|---|---|
| Facebook had the capability to stop the | .836 | | | | |

| | | | | |
|---|---|---|---|---|
| Facebook – Cambridge Analytica scandal from occurring | | | | |
| The Facebook – Cambridge Analytica scandal was preventable by Facebook. | .876 | | | |
| Facebook could have avoided the Facebook – Cambridge Analytica scandal | .895 | | | |
| Facebook should be held accountable for the Facebook – Cambridge Analytica scandal | .703 | | | |
| I have a good feeling about him | | .865 | | |
| I admire and respect him | | .852 | | |
| He has some characteristics I would want to have | | .767 | | |
| I like to learn more about him | | .770 | | |
| I have a good feeling about Facebook. | | | .815 | |
| I trust Facebook. | | | .842 | |
| I admire Facebook. | | | .773 | |
| Facebook has a good overall reputation | | | .846 | |

| | | | | | |
|---|---|---|---|---|---|
| How likely are you going to share the message with other people? (show/forward/retweet) | | | | | .876 |
| How likely are you going to tell your friends about the incident? | | | | | .876 |
| Under most circumstances, I would be likely to believe what Facebook says about the Facebook – Cambridge Analytica scandal | | | | .716 | |
| Facebook is basically dishonest concerning the emission scandal (reversed version), | | | | .828 | |
| I do not trust Facebook to tell the truth about the emissions scandal (reversed version), | | | | .847 | |
| Regarding the Facebook – Cambridge Analytica scandal, Facebook is concerned with the well-being of its publics (e.g., customers, employees, investors) | | | | .542 | |
| Cronbach's a | .85 | .83. | .83 | .71 | .69 |
| Eigenvalue | 2.76 | 2.66 | 2.69 | 2.21 | 1.53 |

**Crisis responsibility**

In order to measure the independent variable of crisis responsibility, the crisis responsibility scale proposed by Brown and Ki (2013) was used. The specific scale is a 7 point Likert scale (1=strongly disagree, 7= strongly agree) with a Cronbach's a value of α= .95 (Brown & Ki, 2013).This scale contains three dimensions to measure crisis responsibility: intentionality, accountability, and locality. The dimensions are comprised of 12 items in total. However, in the locality and intentionality dimension, one item was reduced from each measure, while the dimension of accountability was reduced by two items. Hence, the scale that was used in this study was comprised of eight items in order to be shorter and less repetitive (Wang & Wanjek, 2018). After the reliability test of the new scale, it was discovered that the scale was appropriate for use, as it had a Cronbach's a value of α = .78.

Afterwards, the ten items which were Likert-scale based were analyzed by an exploratory factor analysis using Principal Components extraction with Varimax rotation based on Eigenvalues (> 1.00). The aim of this step was to investigate whether the variable of crisis responsibility was comprised of only one or more dimensions. As the value of Kaiser-Meyer-Olkin (KMO) was .753 and the Bartlett's test for Sphericity was significant, the factor analysis was applicable. After the analysis, three different dimensions were found which verified the Brown and Ki's (2013) theoretical assumption that the scales contained three dimensions: "intentionality", "accountability" and "locality". However, after diving into the results of the factor analysis, the factor that referred to the accountability of the organization towards the scandal was only used, as it explained 69.0% of the variance of the model. The term "accountability", can be translated as the extent to which the public thinks that the organization could have done something to avoid the crisis. This factor contains the following items which were tested on a 7 point Likert scale: "Facebook had the capability to stop the Facebook-Cambridge Analytica scandal from occurring", "The Facebook – Cambridge Analytica scandal was preventable by Facebook", "Facebook could have avoided the Facebook – Cambridge Analytica scandal" and "Facebook should be held accountable for the Facebook –

Cambridge Analytica scandal". Thus, only the items that belonged to the factor of accountability were taken into account and were used in the further analysis.

Additionally, in order to validate that this new dimension which was comprised of 4 items was reliable, a reliability test was conducted which in turn, indicated that the Cronbach's alpha value of the dimension was $\alpha = .85$. Since the value was rather high and the resultant model explained 69.0% of the variance, it was considered suitable for use for further analysis.

**CEO's credibility**

The CEO's credibility scale that was used in this study, was originated from Sohn and Lariscky (2015). These two authors tried to create a scale that would measure the public's evaluation of the CEO, since no other scale was found in academic literature. Hence, the CEO's reputation scale is a combination of North, Desborough and Skarstein's (2005) celebrity scale and Fombrun, Gardberg and Sever's (2000) Reputation Quotient (RQ). There are seven items measuring the attitudes of the audience towards the CEO on a seven-point Likert scale (1 = very strongly disagree, 7 = very strongly agree). However, the scale was narrowed down to 4 items, as it was assumed that only four questions were relevant to measure the attitudes and the credibility towards the CEO. To be more specific, the statements "I believe his opinion to be always right", "I feel a lot of closeness with him" and "Thinking of something good that happened to him puts me in a good mood" were erased from the scale since it was assumed that these statements were rather measuring the worship towards a celebrity and not the credibility. Therefore, the scale was comprised only of the following items: "I have a good feeling about him", "I admire and respect him", "He has some characteristics I would want to have" and "I like to learn more about him". The reliability test indicated that the new scale which included 4 items, was highly reliable and suitable for use, as it had a Cronbach's a value of $\alpha = .83$.

Further, an EFA using maximum likelihood factoring with a Varimax rotation based on Eigenvalues (>1.00) was implemented. Demonstrating a KMO value of 0.789 and having a significant Bartlett's test for Sphericity, the execution of an EFA was

suitable. The results of the factor analysis pointed out that only one factor was found, explaining 66.4% of the variance. Since there was only one factor found by the SPSS there was no rotation and therefore, no Pattern Matrix. This outcome verified that these four items can be considered trustworthy and reliable to measure the effectiveness of the CEO's credibility in this research.

**Pre-crisis reputation**

The public's opinion about Facebook before the scandal was measured on a seven-point Likert scale, indicated by Ponzi, Fombrun and Gardberg (2011). The scale consists of four items: (1)I have a good feeling about Facebook, (2) I trust Facebook, (3) I admire Facebook and (4) Facebook has a good overall reputation. These measures which demonstrate how much the public trusts, admires and likes the company, reported a Cronbach's alpha of $\alpha = 0.96$, based on four divided studies conducted by Ponzi, Fombrun and Gardberg (2011). After testing the reliability of the scale in this research, it was proved that the scale had a Cronbach's a value of $\alpha = .83$ and therefore, was considered reliable for use in this study as well.

Regarding the examination of the correlation between the items within this scale, the KMO value of the model had a value of .790 and the Bartlett's test for Sphericity was significant ($p < .001$), demonstrating that an EFA was applicable to conduct. The EFA of the pre-crisis reputation concept indicated only one factor, which was corresponding with the hypothesis derived from the literature that this scale contained one single dimension. Therefore, no changes were made to this theoretical concept since all items that were included to the dimension had a sufficient factor loading. Lastly, the concept explained 67.2% of the total variance and hence, was assumed appropriate to test.

**Secondary Crisis Communications**

Secondary Crisis Communications was defined as the intentions of stakeholders to tell friends about the crisis, and propagate the information of a crisis online, through

commenting, sharing or informing (Bi, Zheng & Liu, 2014). This dependent variable was measured based on the three indicators proposed by Schultz, Utz & Goritz (2011). Respondents were asked on a five-point Likert scale how likely they are to (a) share the message with other people (show/forward/retweet), (b) tell their friends about the incidents and (c) leave a comment against Facebook on social media. It is important to mention that this section refers to the people's intentions to react to the Facebook – Cambridge Analytica scandal and not to formulate their own opinion.

For this dependent variable, a reliability test was conducted to check the adequacy of the scale that was used based on previous studies. The reliability test indicated that the scale had a Cronbach's a value of $\alpha = .63$. This number signified that the scale was not reliable to a satisfying degree. However, after taken a closer look to the Item-Total Statistics table, it was noted that the elimination of one question ("I am likely to leave a comment against Facebook on social media") could lead to a Cronbach's a value of $\alpha = .69$. Since the value was extremely close to $\alpha = .70$, it was assumed appropriate for use.

For the Secondary Crisis Communications variable, the KMO value was .500 and the Bartlett's test of Sphericity indicated that the model was significant. The analysis proved the existence of only one factor for this model (Table 4.1), while the factor loading of the two items which were included in the factor, was rather satisfactory, as it described in total, 76.7% of the variance.

**Post-crisis reputation**

The Organizational Reputation Scale, created by Coombs and Holladay (2002), was used to measure the reputation of Facebook after the scandal. The scale is comprised of ten items. However, in this case the version of the five – item scale was used. Initially, this scale was created by McCroskey (1966) to measure ethos. The version of the five – item Organizational Reputation Scale had a high Cronbach's alpha value of $\alpha = .87$ and of $\alpha = .81$ in Coombs and Holladay research (2002) and Coombs research (2004) respectively. In the present study, all items were measured by a seven – point Likert Scale (1= strongly disagree, 7 = strongly agree). After conducting a reliability test, it was noted that the scale had a Cronbach's a value of $\alpha = .75$ and thus, was perceived as suitable for this research.

Last but not least, in the EFA, the KMO displayed a value of .648 (df = 10), while the model was significant as indicated by the Bartlett's test of Sphericity. However, two factors were shown in the analysis which marked the existence of two different categories of questions. However, after analyzing the results further, it was found that only 4 items could be included in one factor with a high value of reliability ($\alpha = .71$). Hence, the items that were included in this factor were the following: "Regarding the Facebook-Cambridge Analytica scandal, Facebook is concerned with the well-being of its publics (e.g., customers, employees, investors)", "Under most circumstances, I would be likely to believe what Facebook says about the Facebook-Cambridge Analytica scandal", "Facebook is basically dishonest concerning the emission scandal" (reversed version), "I do not trust Facebook to tell the truth about the emissions scandal (reversed version), "Under most circumstances, I would be likely to believe what the Facebook says about the emissions scandal. The factor loading indicated that the 4 items explained 55.3% of the variance and the variable was considered sufficient to use for the study.

## 5. Results

In this part, the outcomes of the analysis will be discussed. Firstly, the demographic characteristics of the participants will be presented, as well as the respondents' relation with Facebook. After that, the relationship amongst the dependent and independent variables will be analyzed since the reliability of the theoretical concepts and the measurements for each of the independent and dependent variables was already examined in the previous section. Lastly, the six hypotheses will be tested.

### 5.1 Respondents

Out of the total number of the respondents that participated and were included in this research, the majority was women. In fact, 66.5% were female (N = 103) while 32.3% were male (N=50). This could be attributed to the fact that during the time the survey was posted, more females were online, or the groups in which the survey was posted were comprised of more females than males. However, since this research focused on Facebook users globally, it was impossible to control the gender of the users who would participate in the research. The minimum age of the respondents was 18 years old while the maximum was 72 years old. However, the mean age was 32.5 years old (*SD* = 12.03). Regarding the educational level of the sample population, it has to be mentioned that was rather high. 43.2% of the respondents had a Bachelor's degree (N=67), 38.7% had a Master's Degree (N=60) and 7 people out of 155 had completed their PHD. Lastly, 9.7% of the entire sample were graduates of High School (N=15) and 3.9% had graduated from a College Study which was equivalent to Applied Science (N=6). Another demographic characteristic that was taken into account was the nationality of the participants. A total of 38 different nationalities were recorded in this research which points out the global angle of the study. To be more specific, participants were originated from the following countries: USA (*N* = 7), Australia (*N* = 2), Bangladesh (*N* = 1), Bhutan (*N* = 1), Britain (*N* = 13), Bulgaria (*N* = 5), Canada (*N* = 1), Cyprus (*N* = 1), Netherlands (*N* = 14), Egypt (*N* = 1), Estonia (*N* = 1), Germany (N = 4), Greece (*N* = 58), Hungary (*N* = 1), India (*N* = 2), Ireland (*N* = 1), Italy (*N* = 6), Latvia (*N* = 3), Lithuania (*N* = 2), Malaysia (*N* = 1), Montenegro (*N* = 1), Norway (N = 1), Pakistan (N = 1), Peru (N = 1), Poland (N = 2), Portugal (N = 1), Romania (*N* = 2), Russia (*N* = 4), Rwanda (*N* = 1), Sweden (*N* = 1),

Taiwan (*N* = 1), Tanzania (*N* = 1) and Thailand (*N* = 1). However, there were some participants who had more than one nationalities and therefore were categorized as a distinct nationality. To be more specific, there were two people who had a British and Greek nationality, one who had a Greek/American nationality, one who had a Greek/Russian nationality, one with a Polish/Greek nationality and one with a Swiss, French and Danish nationality.

Besides the demographic characteristics of the participants, the survey included questions regarding the relation users have with Facebook. Therefore, there were questions which were asking participants to mention if they ever had a Facebook account, how many years they have been using Facebook and how often they are using Facebook per day. Regarding the first question ("Did you ever have a Facebook account"), 97.4% of the sample answered that they have a Facebook account (N=151), while 4 participants answered negatively. However, they were not excluded from the study since the survey informed them about the Facebook Cambridge Analytica scandal and their opinion was assumed to be useful as well. Regarding the second question which was measuring how many years participants have a Facebook account, the majority of the sample (41.9%) had an account for 7 to 9 years, while 40.6% had an account for 10 years or more. Further, only two participants mentioned that they had a Facebook account for less than a year, while 5.8% and 9.0% of the population had an account for 1 to 3 years and 4 to 6 years respectively. Last but not least, the third controlled variable which was measuring how often participants are using Facebook per day indicated that the highest percentage of people are using Facebook 1 to 3 times (32.9%) or 4 to 6 times (27.2%) per day. 20 participants were recorded to use Facebook less than once per day, while the "heavy" users of Facebook -people who use Facebook more than 10 times per day- were comprised of 24 respondents. To conclude, there were 15 participants who answered that they are using Facebook 7 to 9 times per day.

### 5.2. Correlation and regression analysis

In order to examine the relationship between the variables, the three independent and two dependent variables were entered into a correlation analysis. After that, a regression analysis was conducted with the aim to discover whether the hypotheses of the research

were valid or not. Since the factor analysis that was performed in the previous chapter, is based on correlations, it was presumed that the relationship between the variables was linear, and hence, the correlation and regression analysis could be performed (Pallant, 2007).

The bivariate correlation is used by researchers to examine the strength as well as the direction of the linear relationship amongst multiple variables (Pallant, 2007). In this study, the Pearson's r correlation was used to test the relationship of the variables included in the hypotheses imposed. Pearson correlation coefficients (r) can only take values which fluctuate between +1 and -1. If the sign is positive, it means that when the one variable increases, the other variable increases as well. On the contrary, if the sign is negative, it means that as the one variable increases, the other variable decreases. Furthermore, the strength of the relationship between two or more variables is indicated by the size of the value. If the value is 0, then it is an indication that no relationship exists amongst the variables. Last but not least, in order to define the strength of the correlation between the variables, the guidelines proposed by Cohen (1988) were followed. To be more specific, if the r value is between $r$ =.10 to $r$ =.29, the strength of the relationship is considered small. A medium strength can be underlined, if the Pearson value is between $r$ =.30 to $r$ =.49 and a large strength between variables is indicated when the values are $r$ =.50 to $r$ =1.0. The results of the correlation analysis between the independent variables of CEO's credibility, Pre-crisis Reputation, and Crisis Responsibility and the dependent variables of Post-crisis Reputation and Secondary Crisis Communications can be seen in Table 5.1.

***Table 5.1***.*Correlation analysis between Crisis Responsibility, CEO Credibility, Pre-Crisis Reputation, Post- crisis Reputation, and Secondary Crisis Communications*

| Variables | M | SD | Crisis Responsibility | CEO Credibility | Pre-crisis Reputation | Secondary Crisis Communications | Post-crisis Reputation |
|---|---|---|---|---|---|---|---|
| Crisis Responsibility | 5.15 | 1.12 | - | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| CEO Credibility | 3.91 | 1.28 | -.148 | - | | | |
| Pre-Crisis Reputation | 3.46 | 1.24 | -.253** | .602** | - | | |
| Secondary Crisis Communications | 3.16 | 1.02 | .094 | -.060 | -.113 | - | |
| Post-crisis Reputation | 3.38 | 0.99 | -.349** | .529** | .541** | -.136 | - |

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

Based on the results of the correlation analysis, all independent variables had a significant relationship with the post-crisis reputation of an organization, after a data leak incident. Firstly, there was a significant negative relationship between the independent variable of crisis responsibility and the dependent variable of post-crisis reputation. This means that the more an organization is considered responsible for a cybersecurity incident, the higher will be the reputational loss for an organization ($r = -.35$, $p < 0.001$). Secondly, CEO's credibility had a positive significant relation with post-crisis reputation, and the strength of the relationship was proved rather high ($r = .53$, $p<.001$). This result indicates that an organization will experience less reputational damage, if the CEO is considered highly credible by the public. Last but not least, the relationship between the variables of pre-crisis reputation and post-crisis reputation were also found to be significant and positive, which demonstrates that the higher the reputation an organization has before a crisis, the higher the chances are to experience a small or insignificant reputational damage. Again, the relationship between these two variables was large ($r = .54$, $p < .001$).

Further, regarding the relationship of the Crisis Responsibility, CEO credibility and Pre-crisis Reputation with the dependent variable of Secondary Crisis Communications, the correlation analysis indicated that there was not a significant relationship of the dependent variable with neither of the three independent variables. More specifically, Crisis Responsibility had a significance value of $p$ =.253, CEO

credibility had a value of $p = .495$ and Pre-crisis reputation a significance value of $p = .173$. This means that none of the three variables can be correlated with the engagement and behavior of users on social media in the case of cyber security attacks.

As aforementioned, in order to test the hypotheses of this study, a multiple linear regression analysis was conducted. This type of analysis is based on correlations but enables a more complex and effective investigation of the relationship between a set of variables (Pallant, 2007). In this research, a linear multiple regression was conducted with the following predictors on the dependent variable of post-crisis reputation (Model 1): crisis responsibility, CEO's credibility, and pre-crisis reputation. The model was found to be significant, $F$ (3,124) = 26.04, $p < .001$, $R^2 = .39$. Additionally, a second linear multiple regression was implemented on the dependent variable of Secondary Crisis Communications with the following predictors (Model 2): crisis responsibility, CEO's credibility, pre-crisis reputation. The model in this case was found insignificant, $F$ (3, 125) = 0.41, $p = .746$, $R^2 = .010$. Lastly, two more regression analyses were conducted in order to find out whether the independent variables and the controlled variables (the amount of years people have a Facebook account, the amount of time respondents spend on Facebook per day) and the demographic characteristics (e.g. age, gender, educational level) of the participants' of the study could be proved predictors of the post-crisis reputation (Model 3) and the Secondary Crisis Communications (Model 4). The results of all regression analyses can be found at Table 5.2.

***Table 5.2.*** *Summary of results of all regression analyses*

| **Variables** | **Model 1** (Post-Crisis Reputation as DV) | **Model 2** (Secondary Crisis Communications as DV) | **Model 3** (Post-Crisis Reputation as DV) | **Model 4** (Secondary Crisis Communications as DV) |
|---|---|---|---|---|
| **Independent Variables (IV)** | | | | |

| | | | | |
|---|---|---|---|---|
| *Crisis Responsibility* | -.175* | .046 | -.149~ | .034 |
| *CEO Credibility* | .336*** | -.011 | .373*** | -.047 |
| *Pre-Crisis Reputation* | .292** | -.069 | .270** | -.032 |
| **Controlled Variables** | | | | |
| *Age* | | | .053 | -.164~ |
| *Gender* | | | -.017 | -.001 |
| *Educational Level* | | | -.105 | -.067 |
| *Amount of Years of having a Facebook Account* | | | .017 | .127 |
| *Amount of time spent on Facebook per Day* | | | .110 | -.093 |
| $R^2$ | .387 | .010 | .421 | .060 |
| *F* | 26.04 | .410 | 10.532 | .927 |
| *N* | 155 | 155 | 155 | 155 |

Notes: Reported effects are standardized (Beta) coefficients.

Significance levels: : ~ $p < .10$ *$p < .05$ ** $p < .01$ *** $p < .001$.

### Hypothesis 1a.

The first hypothesis imposed in the research concerned the impact of the CEO's credibility on the post – crisis reputation of an organization, after a cybersecurity incident. It was assumed that organizations which have a trustworthy and credible CEO would not suffer from reputational loss after the incident since the stakeholders will be influenced by their trust and admiration towards the CEO of the company. The linear multiple regression analysis indicated that the CEO's credibility is a significant predictor

to the model ($b$ =.34, $t$ = 3.82, $p$ < .001). Post-crisis reputation increased by 0.34 (on a 7 point Likert scale in which 1 was negative and 7 was positive) for every point rise in the CEO's credibility. This means that indeed, corporations who have a CEO who is trusted and is regarded credible by the public, have the power to influence the public's opinion and it is possible that they will suffer less reputation damage after a data leak incident. Thus, the hypothesis was verified.

**Hypothesis 1b**.

This hypothesis speculated that the CEO's credibility will have a negative relationship with the behavior of users online after a cybersecurity crisis. This means that when the public trusts and admires the CEO of an organization, individuals will be less likely to tell or talk about the cyber security incident with their friends or show, forward and retweet a post that has information regarding the incident. In the linear multiple regression analysis, the CEO's credibility was found to be an insignificant predictor ($b$ = -.01, $t$ = -0.10, $p$ = .919). Hence, the null hypothesis was confirmed, which means that whether the inspired credibility of the CEO by the public is low or high, this variable has no impact on the behavior of users online to inform, react, or share content regarding the crisis incident with their friends or their network.

**Hypothesis 2a.**

The first hypothesis regarding the impact of the pre-crisis reputation on the post-crisis reputation of an organization presumed that these two variables will have a positive and significant relationship. To be more specific, it was hypothesized that if an organization has a strong reputation prior to a cybersecurity crisis, this fact will have a positive effect on its post-crisis reputation, meaning that the organization will not experience a great reputational loss. Based on the linear multiple regression analysis, the pre-crisis reputation was found to be a significant predictor ($b$ = .29, $t$ = 3.25, $p$ = .001). For every point increase in Pre-crisis Reputation, the Post-crisis Reputation was increased by 0.29. Consequently, when a data leak incident occurs, a favorable reputation prior to the crisis is considered important for an organization, since it was proved that it can prevent a

damage to the reputation of a company after the incident. This means that the hypothesis of the present study was confirmed.

**Hypothesis 2b.**

The second hypothesis that was formulated regarding the variable of pre-crisis reputation, focused on its impact on the behavior of the public online after a cyber security incident. Therefore, it was expected that the public will not "spread the message" of the crisis on social media and any digital platform, if the pre-crisis reputation of the organization is high. According to the results of the linear multiple regression analysis, the variable of pre-crisis reputation was found to be an insignificant predictor ($b$ =-.07, $t$ = -0.607, $p$ = .545). Consequently, this hypothesis was rejected and the null hypothesis was accepted. The null hypothesis, in this case, assumed that the reputation of an organization before a crisis, whether it is high or low, will not have an effect on the willingness of users to talk about the crisis or forward messages regarding the crisis on social media.

**Hypothesis 3a.**

The first hypothesis of the third part, assumes that in the incident of a cyber security crisis, the amount of responsibility that will be attributed to the organization by the public, which is experiencing the crisis, will have a negative impact on the reputation after the crisis. Based on the results of the multiple linear regression analysis, it can be seen that crisis responsibility can be proved a significant predictor of the post-crisis reputation of a corporation after a cyber security incident ($b$ = -.18, $t$ = -2.41, $p$ = .017). Post crisis reputation decreases with -.175 (on a 7 point Liker scale, when 1 is negative and 7 is positive) for every point increase in Crisis Responsibility. This means that organizations who are going through a cyber security crisis, should pay more attention to who the public perceives as responsible for the incident as the results indicated that individuals' perceptions regarding the accountability of an organization during a crisis, can have significant consequences to the reputation of the organization after the data leak incident.

**Hypothesis 3b.**

The second hypothesis concerning the impact of the crisis responsibility on the behavior of users online claims that, when a cyber security incident occurs and people blame the organization at a high degree, they will be more likely to "spread the message" of the crisis on social media by forwarding, sharing or retweeting relevant content. The linear regression analysis indicated that the crisis responsibility contributed only 4.2% to the prediction of the dependent variable ($b$ = .05, $t$ = 0.50, $p$ = .619). However, the second hypothesis was rejected as the model was insignificant. Once again, the null hypothesis was verified, meaning that people's behavior on social media and their willingness to talk about the incident with their friend can't be influenced by their perception on whether the incident was a purposive act by the organization or not.

### 5.3 Further findings

Although the research question of this study focuses on the impact of the three aforementioned independent variables (CEO's credibility, crisis responsibility, pre-crisis reputation) to the reputation of an organization after a data leak incident, as well as to the behavior of users on social media directly after the outbreak of a data leak incident, a variety of other independent variables were also tested whether they have an impact on the two dependent variables. Therefore, a second regression analysis was conducted on post-crisis reputation and on secondary crisis communications. The aim of this action, was to test whether other controlled variables, such as demographics (gender, age and educational level), the amount of years that an individual has a Facebook account or the amount of time that a person uses Facebook per day can also play a role on influencing their perception towards an organization, or their intention to use social media after a data leak crisis.

#### Additional results on post-crisis reputation

The first linear multiple regression analysis included the following variables as independent variables except of the CEO credibility, Crisis Responsibility and Pre-crisis Reputation towards the dependent variable of post-crisis reputation: the amount of years someone has a Facebook account, the amount of time the individuals spend on Facebook, gender, education level and age (Table 5.2, Model 3). The model of the regression

analysis was significant, $F$ (8, 116) = 10.53 ($p < .001$, $R^2 = .42$). Gender and educational level were found to have a negative relationship with post-crisis communication which means that women were less likely to "punish" and stop their relationship with an organization after a crisis. This may mean that women are more emotional and attached to an organization, but since no emotions were tested as mediators in this study, this conclusion can only be a speculation. Regarding the educational level, the regression analysis indicated that people with high education are expected to cause a greater reputational loss to an organization from people who are less educated. However, both variables were found to be insignificant as gender indicated a significance of $p = .819$ ($b = -.02$) and educational level a significance of $p = .161$ (b = -.11), and therefore were not considered as predictors of post-crisis reputation.

Interestingly, none of the other independent variables seemed to have a significant relationship and impact on the post-crisis reputation of the organization. This proves that age ($b = .05$, $p = .471$), the amount of time individuals spend on Facebook ($b = .11$, $p = .145$) and the amount of years respondents use Facebook ($b = .02$, $p = .826$) cannot predict the reputation of an organization after a cybersecurity crisis.

**Additional results on Secondary Crisis Communications**

The second linear multiple regression analysis focused on finding a possible relationship between the depended variable of Secondary Crisis Communications and the following dependent variables: the amount of years someone has a Facebook account, the amount of time the individuals spend on Facebook, gender, education level and age (Table 5.2, Model 4). Since crisis responsibility, CEO credibility and pre-crisis reputation were proved to be insignificant predictors of the behavior of users on social media, the aim of this regression analysis was to identify if another variable could predict or foresee the intention of people to talk or forward the message of the crisis on social media. The model of the regression analysis was again insignificant, $F$ (8, 117) = .93, $p = .497$, $R^2 = .06$.

Consequently, none of the independent variables seemed to be a determinant predictor on the post-crisis reputation of the organization. This proves that age ($p = .082$,

*b* = -.16), gender (*p* = .994, *b* = -.001), the amount of years that the respondents are having a Facebook account (*p* = .182, b = .13), the amount of time individuals spend on Facebook (*p* = .323, *b* = -.09) and the educational level (*p* = .480, *b* = -.07) are not correlated and cannot impact the reputation of the organization after a data leak incident.

## 6. Discussion

In this chapter, the outcomes of the data analysis will be interpreted and discussed within the theoretical concepts that were mentioned earlier in chapter 2. Further, the contributions of this study in the crisis communication theories will be demonstrated, as well as the theoretical implications. Lastly, advices will be given to people who are responsible for the assessment and dealing of cyber security crises.

To begin with, this research was based on two theoretical frameworks: the SCCT and the SMCC. The former model is providing guidelines to organizations and especially to crisis communication managers on how to assess and handle a crisis situation during and after a crisis. It also provides insights on which are the ideal response strategies based on the type of crisis each organization is experiencing in order to minimize the threat of an incident to the reputation of an organization. The second model that was used for this study, provides details on how social media and other online digital platforms can be incorporated into the crisis communication context, as in this day and age social media constitute a big and essential part of individuals' daily routine (Leung & Lee, 2005). By combining these two frameworks, it can be stated that the innovatory element of this study was thus, the effort to develop a more complex perspective on crisis communication. This attempt focused on taking into consideration the crisis type and the variables that have an impact not only on the reputation of an organization after a crisis but also on the interactive relationship of users and stakeholders on social media and their willingness to forward to message of a crisis. Additionally, as the public performs all of its daily activities through digital applications and social media, this research desired to add value to the crisis communication literature by examining a more current and significant type of crisis that has a great impact on people's lives, which is the cyber security attacks and the harvesting of users' personal and intimate information.

The first variable that was tested was crisis responsibility and its effect on post-crisis reputation. According to the SCCT theory, when a crisis emerges, people instantly attribute a degree of blame to the organization that is involved in the crisis and this has a significant impact on the reputation of the organization after the crisis (Coombs, 2007; Weiner, 1985).The results of this study indicated that in fact, crisis responsibility is

correlated with the post-crisis reputation of an organization in the case of cyber security incidents. Therefore, it was found that the SCCT model can be applied to a new type of crisis, the one of data leaks. Additionally, the authors of the theory stated that when individuals blame the organization on a high degree, then the latter will experience a great reputational loss. In the case of the Facebook-Cambridge Analytica scandal, people attributed a high accountability to Facebook for the scandal. Based on these results, it would be logical to assume that Facebook would have had a rather high reputational loss, as the scandal was considered as an intentional act and not an accident. Interestingly, the majority of people in the study who thought that Facebook-Cambridge Analytica scandal was an act that could be avoided by Facebook, indicated the same time that, they still haven't totally lost their trust and support to Facebook. When interpreting these findings though, it should be taken into account that the crisis responsibility scale was narrowed down to less items during the data analysis. Therefore, when examining the Facebook's crisis responsibility for the scandal in this study, it does not refer to intentionality, which can be translated to the degree to which the crisis occurred due to an intentional act by a member or more of the organization, nor to locality, meaning the degree to which the crisis was an internal matter. The crisis responsibility in this case only stands for the extent to which Facebook could have avoided the incident. Thus, the majority of the respondents believed that the data leak incident was a crisis that could have been avoided by Facebook and that Facebook should be held responsible for this incident.

After diving deeper into these results, it should be also taken into account that according to Coombs (2007), in order to assess the reputational threat of a crisis, crisis responsibility is not the only element that should be measured. In fact, in the SCCT model, it is mentioned that the crisis history of a company plays a pivotal role when assessing the threat of a crisis. Consequently, the fact that Facebook has not been accused of a data leak incident before, may have played a fundamental part in the degree in which the reputation of Facebook was affected. Individuals may thought that since this was the first incident of a cyber security attack that Facebook was involved, the organization may had had the power to prevent the crisis, but they also gave it the benefit of the doubt. Another explanation might be that the public focused more on how to overcome this

crisis, rather than terminate their relationship with Facebook. An additional assumption that could also explain these results, could be the fact that this study was conducted one year after the incident which can be considered as a long gap between the incident and the conduct of the research. According to Coombs and Holladay (2007), emotional responses could decrease over time because the stakeholders forget about a crisis. Therefore, people probably still had an opinion whether Facebook was accountable about the Facebook – Cambridge Analytica scandal, but one year later their emotions were not that strong in order to express a hostile opinion towards the organization.

Moreover, when interpreting the results, another element that pertains to the assessment of the reputational damage of a crisis to an organization should be taken into account. According to several authors, the effect of the prior relational reputation a company has, is the most significant predictor when managers are trying to assess the reputational damage of an organization and is regarded more essential for the reputation of organizations during crisis than crisis history (Coombs & Holladay, 2001; Sheldon & Sallot, 2009). The pre-crisis reputation of Facebook was tested in this study, and the results indicated that it was modest but a significant predictor of post-crisis reputation. This means that the perceptions of the public after the crisis towards the organization were affected by their view of the organization before the incident. Hence, individuals were probably of the opinion that, until now the organization was taking into account its stakeholders to a satisfying way and they showed trust to the organization. In this case then, the assumption that a favorable pre-crisis reputation towards an organization can function as a halo effect can be verified. Previous studies which have examined the existence of the halo effect, have claimed that only organizations with very favorable prior reputation can experience the halo effect (Coombs & Holladay, 2006). Since Facebook is proved to be one of the most used social media globally, it should be expected that its pre-crisis reputation would be rather high. However, it was proved moderate, but the fact that its post-crisis reputation in this study was also moderate, may add value to the halo effect theory and prove that organizations which have a moderate pre-crisis reputation can also experience the advantages of a favorable reputation as a shield for their organization. Another theory that can be verified is the function of a

favorable reputation as a "capital". As mentioned earlier in this study, Facebook is one of the most used social media worldwide and amongst all ages. Therefore, when the scandal occurred, Facebook spent a large amount of its "reputational capital" and this was the reason why even though stakeholders put the blame on the organization, the organization remained strong and wasn't affected by the crisis. However, these interpretations are just assumptions and are based on the interpretation of the researcher. Last but not least, the theory that highlights how a favorable pre-crisis reputation can function as a "boomerang" to an organization after a crisis was rejected. This theory could only be proved if the pre-crisis reputation was modest or high, but the post-crisis reputation was low.

Furthermore, the statistical medium mean of post-crisis reputation of this study may also be attributed to the response strategy of Facebook. As mentioned in the news, the CEO of Facebook, Mark Zuckerberg, who was speaking on the behalf of his organization, admitted that he should be accounted as responsible for the incident and he apologized to all Facebook users, globally, through a letter and a post on social media. Hence, the respondents of the study may have been also influenced by the type of the response strategy that the CEO of Facebook used. Coombs and Holladay (2008) have found that apology as a response strategy can be proved effective to stakeholders who are not victims of the crisis and probably this could be an explanation of why respondents still trust the organization to a medium degree. However, since the present study didn't test the effect of the response strategy, this argument cannot be considered as valid but only be taken into account as an assumption.

One last interpretation of the results could be embedded to a cultural factor. Previous research in risk and crisis management has indicated that people evaluate a risk or a crisis based on their own personality. According to Pidgeon & Henwood (2010) "portrayal (of risk) in mediated and other sources interact with psychological, social, institutional, and cultural processes in ways that might attenuate (decrease) or amplify (increase) perceptions of risk, and through this, shape behavior" (p. 54). This can be called cultural bias which it can be classified to individualism and collectivism (Dake & Wildavsky, 1991). Therefore, when a crisis emerges, individualists seek to maintain

independence from others and are not affected by the public's opinions or feelings. Since the Facebook – Cambridge Analytica scandal affected only the American people, whereas the sample of this study had mostly participants from other countries, it can also be claimed that in the case of data leaks, when people are not affected personally, there is a chance that they still trust to a moderate degree the organization, even though they consider it accountable for the incident.

A key finding of this research was the significant role of the CEO during a crisis. Previous research has focused on the essential role of the CEO in handling crises effectively (Alsop, 2004; Fombrun, 1996; Griffin, 2008) and whether the CEO is the person who should be the spokesperson of an organization during and after a crisis (Turk et al., 2012). However, no empirical evidence were found in the literature regarding the effect of the CEO as a credible and celebrity persona to the corporate reputation of an organization after a cyber security crisis. As Van Riel and Fombrun (2007) stated, CEOs play a significant role as the "spiritual and emotional leaders of the organization" (p.16), and therefore there is an increasing need in identifying the role of a CEO as a celebrity and its impact to his/her stakeholders. Therefore, this study added value to the significant role of the CEO and the credibility he inspires to the public, as part of an organization and especially as part of dealing with a cybersecurity crisis. In this research, it was proved that attitudes towards the CEO can have a positive impact on the reputation of an organization after the crisis. Even though the CEO's credibility was rather modest, the CEO's impact in cyber security crises was verified. This result can confirm the assumption that sometimes the CEO's reputation and fame can be considered as more important than the reputation of the company during a crisis (Flatt et al., 2013; Turk et al., 2012). This means that indeed, people pay attention to the characteristics, the history and the fame of the CEO of a company and probably identify the persona of the CEO as a celebrity with the organization, which makes them more vulnerable towards the CEO's perceptions and statements about a crisis. Moreover, since the post-crisis reputation of Facebook wasn't affected to a high degree, even though it was considered as an intentional act, may prove the theory that CEOs have the power to direct people's

perceptions on a crisis and even inspire a sense of control, since they are deemed as the representatives of the organizations.

Since cyber security incidents are a new type of crisis, it was found essential that they should be examined within the new environment that crisis communication is operating, and this is the digital world and more specifically the world of social media. The aim of this act was to identify the predictors which influence people's intention to propagate a crisis on social media, since the use of social media can be proved unforeseeable and dangerous for organizations who are experiencing a crisis. Information is disseminated and shared to users in such a speed rate, that no organization is able to handle this situation. Therefore, it was considered as an astute idea to test which elements influence people's behavior online, in order to give organizations a guideline on what to expect when a cyber security crisis emerges. Interestingly, the SCCT model in this case was not proved helpful. Neither the independent variable of crisis responsibility, nor the independent variables of CEO's credibility and pre-crisis reputation seemed to be significant predictors of people's engagement with social media. Additionally, other characteristics of the users were also tested as predictors (e.g. age, gender, educational level, amount of time spent on Facebook and amount of years respondents had a Facebook account), but unfortunately none of them was proved as a significant indicator again. However, it must be mentioned that these independent variables have not been tested to a high degree by other researchers. Until now, three big themes have been identifying regarding their impact on the behavior of users online and their willingness to propagate the message of the crisis and these are the following: (a) the response strategies and their effect on Secondary Crisis Communications (Bi et al., 2014), (b) the influence of the source of message via which individuals receive information about a crisis (Austin et al., 2012; Jin & Liu, 2010) and (c) the fluctuation of people's use of social media right after a crisis occurs (Lariscy, Avery, Sweetser, & Howes, 2009). In these cases, it was found that some responses and message sources were significant predictors of people's engagement with social media. However, a further research must be conducted in order to test other independent variables or mediators and their relation with the engagement of users online, such as crisis history and emotions.

### 6.1 Managerial implications

The outcomes of this study, as well as their interpretation, can lead to several practical suggestions in the context of crisis communication in cybersecurity incidents. First and foremost, as it was revealed in this research, crisis responsibility is a significant predictor of the reputation of an enterprise after a data leak incident. This means that managers who are responsible for crisis management and communication should initially assess how the public perceives the crisis and whether their organization is regarded as accountable for the incident or not. This act will ultimately help them to recognize which crisis response is more suitable to use in order to avoid a great reputational damage and convince the public that the crisis is either under control or is being handled by the organizations. In any case though, as mentioned in the literature, the organizations should give a guideline to their customers or their general stakeholders on how to overcome and handle the situations as being victims by a cybersecurity attack. Additionally, taking as an example the Facebook-Cambridge Analytica scandal, it should be taken into account that there are some factors who can influence the public's behavior and perception towards an organization, even though the public attributes high responsibility to the organization.

Another practical suggestion based on the outcomes of the study concerns the pre-crisis reputation of an organization. As the results indicated, organizations with a favorable pre-crisis reputation can experience a medium reputational loss after a cybersecurity incident. People who are responsible for the crisis communication of an organization, or even the personal relations of it, should pay great attention to building a strong and reliable brand. Organizations whose stakeholders believe that they receive a high quality of services and that the former is taking into account their well-being, safeguard their identity and protect them against any hacking event, will be more likely to give the organization the benefit of the doubt when a crisis like this emerges. Therefore, building upon the relationship with customers should be a high priority for organizations that may experience a data leak incident. Lastly, since every corporation nowadays is operating online and the majority of them have probably a database with all their clients'

personal information, this kind of crisis should be taken seriously and into account by all kind of organizations, regardless the industry they operate.

Another key finding of this research was the influence that celebrity CEOs have towards the opinions of the public. This study found that the perception towards the CEO of an organization can play a significant role during a crisis as it can affect the public's perceptions and opinions in relation to the crisis. Therefore, enterprises should aim at creating a strong profile of their CEOs in the public sphere. Previous literature has mentioned that numerous times, CEOs are not exposed to the public when a crisis occurs for two main reasons. The first reason is due to the opinion of the CEOs of the company that he/she should focus on working effectively at the office to combat the crisis event and not spend time appearing at the media (Griffin, 2008). The second reason lies upon the decision and the perception of several crisis communication managers that CEOs cannot be regarded as a credible source for the public as people tend to attribute more blame to someone who is regarded as wealthy and powerful (Vidmar, 1993). On the contrary, this research indicated the importance of the CEO's credibility during cybersecurity incidents. However, this credibility can only be built if people who are working in the industry of public relations pay more attention to create a strong and reliable profile of their CEOs, similarly with the one of celebrities. In addition, since the public seems to count on the fame that a CEO has, managers of crisis communication should not only focus on creating a credible profile of their CEOs but also encourage them to be the spokesperson of the corporation in case of crises. By doing so, there is a great probability that people will identify the image of the CEO and his/her credibility with the one of their organization's and the latter will be more likely to experience less reputational loss. On the contrary, if the CEO of an organization is not known to the public, maybe another person to handle the crisis must be more appropriate.

Unfortunately, this study could not find any predictor of people's behavior on social media, directly after a crisis emerges. Therefore, no recommendations can be made to managers of crisis communication on how to foresee the reaction of the public and their willingness to propagate the message of a crisis through the use of their social media

accounts. However, this fact can also be attributed to the limitations of this study which will be presented in the next chapter.

## 7. Conclusion

The purpose of this study was to examine the impact of the independent variables of the CEO credibility, crisis responsibility and pre-crisis reputation to the dependent variables of post-crisis reputation and secondary crisis communications in the crisis context of cyber security attacks. Data leak and cybersecurity attacks in general, are a new form of crisis that all organizations are facing nowadays and have detrimental ramifications to the reputation of the organizations and most importantly to their customers, as their intimate and personal information is harvested by third unknown parties (Philips, 2002; Veltsos 2012). However, not only the type of crisis is new, but also the way that the crisis message is propagating through the public. In the past, organizations had the opportunity to send information to the public regarding a crisis, and this information was up to a degree controlled by the corporations. Therefore, there was a one-way communication with the public, in which the public could only receive details about the crisis and talk about the incident with their network (Coombs & Holladay, 2014). With the rise of social media, the relationship between the organization and the stakeholders during a crisis was altered, since these digital platforms enabled individuals to share their experiences, emotions, and opinions online. In this context, this study found it vital to examine the drivers of people's behavior and engagement on social media during crises, as social media constitute one of the main tools for individuals to communicate and interact not only with their close network but also with people with same interests and concerns. It was thus, assumed that conducting a research within this framework, would give a great insight to researchers and managers of crisis communication on how to protect their organization and what to expect from people's behavior on social media.

The results of the study indicated that theories which apply to the crisis communication literature, such as SCCT can also be proved fruitful in the case of data leaks. More specifically, two elements of this model were found to be significant predictors of the post-crisis reputation of an organization. These are the crisis responsibility attributed by the public and the pre-crisis reputation. Additionally, a new component was discovered as an indicator of the post-crisis reputation of an organization: the CEO's credibility. However, this study was unable to find a significant determinant of

what leads people to use social media directly after a cybersecurity crisis and what triggers them to propagate content to their friends and their network regarding the incident.

### 7.1 Strengths and limitations of the study

This study contributed to the existing literature of crisis communication, as it proved that the SCCT model can also be applied in the case of cybersecurity crises. Although the model was formulated almost a decade ago, it was proved beneficial for use in order to assess the threat of this type of crisis. More specifically, the results of the study indicated that at least two predictors of the SCCT model are significant predictors of the post-crisis reputation of an organization and these are the crisis responsibility and the pre-crisis reputation of the organization. Most importantly, this study can be considered as insightful and valuable for crisis communication as it added one more predictor of the public's perception towards an organization after a data leak, and this is the role of the CEO and the credibility he/she inspires. Thus, not only crisis responsibility and pre-crisis reputation as proposed by Coombs and Holladay (2014), but also CEO's credibility can play a pivotal role in foreseeing the reputational damage of an organization in the context of cybersecurity crisis.

Moreover, the present study added value to existing research by applying a quantitative method in the context of crisis communication through the use of a survey. Therefore, it went beyond the use of case studies which were aiming at testing the effect of different dependent variables on the post-crisis reputation of organizations which had been dominating the field of crisis communication.

However, there are certain limitations of this research that should not be neglected. To begin with, the first limitation of the present research, is dealing with the methodology used to derive and analyze data. On the one hand, the use of a quantitative method through a survey might have been a new approach of research for the crisis communication field and in general, quantitative methods are considered as a valuable method in order to test big samples. However, when interpreting the data, surveys put some boundaries to the researcher when trying to go more in depth in the results of the

study. For instance, as mentioned in the previous chapters, individuals attributed a high degree of responsibility to the organization, but the post-crisis reputation of the organization was not affected to the same degree. In order to interpret these kind of results, a more in depth research must be conducted. More specifically, the use of interviews could be an efficient solution if researchers want to identify the motives of people's behavior and explain results that are not easy to interpret only by using quantitative data. Hence, in the present study, the underlying reasons behind these types of behavior cannot be interpreted in an effective way, since only assumptions can be made based on previous findings.

Furthermore, as mentioned in previous chapters, the SCCT model was used in order to assess the threat of the cybersecurity crisis. However, only two elements of this theory were used and these are the crisis responsibility and the pre-crisis reputation. Therefore, it cannot be stated for sure if this model is a perfect fit or not for examining cybersecurity crises. In order to state this argument for sure, other independent variables such as the crisis history of the organization and the response strategy should also be taken into consideration. Then, the assessment of the crisis can be conducted properly and examine whether the whole model is indeed suitable for examining the cybersecurity crises.

Another limitation of the study can focus on the sample size of the study and the characteristics of the respondents. The present research only received data from 155 users of Facebook. If the total number of Facebook users is taken into account, it can be stated that 154 users are a really small sample and thus, cannot be regarded as representative. Additionally, the sample is comprised of mostly young and highly educated participants which means that these results could be different if there was an equal amount of respondents that would represent young and older people and highly as well as less educated people. Another point worth mentioning is the nationalities of the participants. As it was mentioned in previous chapters, the sample indicates that there is a variety of nationalities involved in this study. However, if we go more in depth in this data it could be noticed that although there is a variety of people representing different countries, the number of respondents from each country is usually one to three respondents. There were

only few countries that included more than three participants which means that it may give a global angle to this study, but at the same time, the amount of respondents from each country is not sufficient. Consequently, this bias needs to be taken into consideration when interpreting the results of this study.

### 7.2. Future research

After taking into account the strengths as well as the limitations of the present study, there are several suggestions for further research to researchers who are interested in the field of crisis communication, and especially investigating the cyber security attacks.

Firstly, as it was known by the introduction of this study, Facebook – Cambridge Analytica scandal was an incident that only affected American users of Facebook, as the ultimate goal of this scandal was to harvest personal information from American users in order to foresee their vote in the American Presidential Elections in 2016. Therefore, it would be fruitful if this study could be replicated there, in order to investigate the behavior and perception of people who were actually victims of this crisis. Within this context, however, it would also be very insightful if future research could focus on identifying possible behaviors between people who were actually affected by the crisis, and people who are Facebook users but the scandal didn't cause any harm to them. In this case, another type of sampling method should be applied. In order to generalize results, a non-probability sampling could be used such as quota sampling. This method would facilitate researchers to include individuals with specific characteristics that are relevant for the study and therefore, the sample would be less biased (Babbie, 2011). In the present study, the use of convenience sampling was applied due to the fact that it was rather difficult to reach above 150 respondents in another way. In both cases, however, it must be mentioned that a greater number of a sampling size should be used, as this study couldn't reach more than 155 participants.

Moreover, future studies on cybersecurity crises could include other independent or dependent variables that have not been considered in the present study such as crisis history, response strategies, and secondary crisis reactions. Regarding the latter,

secondary crisis reactions differ from the secondary crisis communications as they represent the intended behaviors of the public to either support or criticize and condemn the organization involved in the crisis. In the case of secondary crisis reactions this can be translated as their willingness to boycott a corporation and also persuade others to do so through online and offline word of mouth (Schultz, Utz & Göritz, 2011).

Last but not least, future research should also focus on identifying the drivers of Secondary Crisis Communication online, in the case of cyber security incidents. This study tried to approach a more complex perspective of crisis communications and incorporate the drivers that influence the willingness of stakeholders to forward the message of the crisis on social media. However, no significant predictors were found that could foresee people's intention to tell their friends about a cybersecurity incident or forward the message through a post or a retweet. Therefore, it is of utmost importance to identify these motives, as the behavior of people on social media can be unpredictable and a great threat to organizations who are experiencing a crisis.

## 8. References


Alghawi, I. A., Yan, J., & Wei, C. (2014). Professional or interactive: CEOs' image strategies in the microblogging context. *Computers in Human Behavior, 41*, 184-189. doi:10.1016/j.chb.2014.09.027

Alsop, R. J. (2004). Corporate reputation: Anything but superficial – the deep but fragile nature of corporate reputation. *Journal of Business Strategy, 25*(6), 21-29. doi:10.1108/02756660410699900

Ashley, C., & Tuten, T. (2015). Creative strategies in social media marketing: An exploratory study of branded social content and consumer engagement. *Psychology and Marketing, 32*(1), 15-27. doi: 10.1002/mar.20761

Austin, L., & Jin, Y. (2016). Social media and crisis communication: Explicating the social-mediated crisis communication model. In A. Dudo & L. A. Kahlor (Eds.), Strategic Communication: New Agendas in Communication (pp. 164–186). Retrieved from https://www.researchgate.net/publication/316488296_Social_media_and_crisis_ommunication_Explicating_the_social-mediated_crisis_communication_model

Austin, L., Liu, B. F., & 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. doi:10.1080/00909882.2012.654498

Avery, E. J., Lariscy, R. W., Kim, S., & Hocke, T. (2010). A quantitative review of crisis communication research in public relations from 1991 to 2009. *Public Relations Review, 36*(2), 190-192. doi:10.1016/j.pubrev.2010.01.001

Babbie, E. R. (2011). *Introduction to social research*. Wadsworth: Cengage Learning.

Benoit, W. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177-186. doi: 10.1016/s0363-8111(97)90023-0

Bi, G., Zheng, B., & Liu, H. (2014). *Secondary Crisis Communication On Social Media:The Role of Corporate Response and Social Influence in Product – Harm*

*Crisis.* Retrieved January 15, 2019, from https://aisel.aisnet.org/pacis2014/93/?utm_source=aisel.aisnet.org/pacis2014/3&utm_medium=PDF&utm_campaign=PDFCoverPages.

Brown, K.A., and E.J. Ki. 2013. Developing a valid and reliable measure of organizational crisis responsibility. *Journalism & Mass Communication Quarterly, 90*(2), 363–384. doi: 10.1177/1077699013482911.

Brubaker, P. J., & Haigh, M. M. (2017). The Religious Facebook Experience: Uses and Gratifications of Faith-Based Content. *Social Media Society, 3*(2). doi: 10.1177/2056305117703723

Caponigro, J.R. (2000), *The Crisis Counselor: A Step-by-Step Guide to Managing a Business Crisis*. Chicago: Contemporary Books.

Carroll, C. (2009). Defying a Reputational Crisis – Cadbury's Salmonella Scare: Why are Customers Willing to Forgive and Forget? *Corporate Reputation Review, 12*(1), 64-82. doi: 10.1057/crr.2008.34

Choi, Y. & Lin, Y.H. (2009). Consumer Responses to Mattel Product Recalls Posted on Online Bulletin Boards: Exploring Two Types of Emotion. *Journal of Public Relations Research,* 21(2), 198-207. doi: 10.1080/10627260802557506

Claeys, A., & Cauberghe, V. (2015). The role of a favorable pre-crisis reputation in protecting organizations during crises. *Public Relations Review, 41*(1), 64-71. doi:10.1016/j.pubrev.2014.10.013

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. Retrieved December 25, 2018, from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica scandal-fallout.html

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. doi: 10.1177/089331802237233

Coombs, W.T. & Holladay, S. J. (2006). Unpacking the halo effect: reputation and crisis management. *Journal of Communication Management, 10*(2), 123-137. doi: 10.1108/13632540610664698

Coombs, W. T. (2010). Parameters for crisis communication. In W. T. Coombs & S. J. Holladay (Eds.), *The handbook of crisis communication* (pp. 17-53). Malden, MA: Blackwell.

Coombs, W.T. & Holladay, S.J. (2008). Comparing apology to equivalent crisis response strategies: Clarifying apology's role and value in crisis communication. *Public Relations Review, 34*(3), 252- 257. doi: 10.1016/j.pubrev.2008.04.001

Coombs, W. T., & Holladay, S. J. (2012). Amazon.com's Orwellian nightmare: Exploring apology in an online environment. *Journal of Communication Management, 16*(3), 280-295. doi: 10.1108/13632541211245758

Coombs, W. T., & Holladay, S. J. (2014). How publics react to crisis communication efforts. *Journal of Communication Management, 18*(1), 40-57. doi:10.1108/jcom-03-2013-0015

Dean, D. H. (2004). Consumer reaction to negative publicity effects of corporate reputation, response, and responsibility for a crisis event. *Journal of Business Communication, 41*(2), 192-211. doi: 10.1177/0021943603261748

Dudo, A., & Kahlor, L. (2017*). Strategic communication: New agendas in communication*. New York: Routledge.

Edwards, K., & Smith, E. E. (1996). A disconfirmation bias in the evaluation of arguments. *Journal of Personality and Social Psychology, 71*(1), 5-24. doi:10.1037/0022-3514.71.1.5

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4. doi:10.11648/j.ajtas.20160501.11

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research, 15*(2), 195-219. doi:10.1108/10662240510590360

Fetscherin, M., Gaines-Ross, L., & Bates, S. (2015). *CEO branding: Theory and practice.* New York: Routledge.

Fombrun, C. J. (1996). Reputation: Realizing value from the corporate image. Boston, Mass: Harvard Business School Press.

Fombrun, C. J., Gardberg, N. A., & Sever, J. M. (2000). The Reputation QuotientSM: A multi-stakeholder measure of corporate reputation. *Journal of Brand Management, 7*(4), 241-255. doi:10.1057/bm.2000.10

Fombrun, C.J. & van Riel, C.B.M. (2004). *Fame & Fortune: How Successful Companies Build Winning Reputation.* New York: Prentice-Hall Financial Times.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security, 46*, 18-31. doi:10.1016/j.cose.2014.06.008

Fraustino, J. D., Liu, B. F., & Jin, Y. (2012, December). Social media use during disasters. Report submitted to the National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. Retrieved June 2, 2019, from https://www.start.umd.edu/sites/default/files/files/publications/START_SocialMediaUseduringDisasters_LitReview.pdf

Gramlich, J. (2019, February 1). 10 facts about Americans and Facebook. Retrieved April 13, 2019, from https://www.pewresearch.org/fact-tank/2019/05/16/facts about-americans-and-facebook/

Griffin, A. (2008). New strategies for reputation management: Gaining control of issues, crises and corporate social responsibility. Philadelphia, PA: Kogan Page Ltd

Grunwald, G., & Hempelmann, B. (2010). Impacts of Reputation for Quality on Perceptions of Company Responsibility and Product-related Dangers in times

of Product-recall and Public Complaints Crises: Results from an Empirical Investigation. *Corporate Reputation Review, 13*(4), 264-283. doi:10.1057/crr.2010.23

Heverin, T., & Zach, L. (2010, May). Proceedings of the 7th International ISCRAM Conference. *In Microblogging for Crisis Communication: Examination of Twitter Use in Response to a 2009 Violent Crisis in the Seattle-Tacoma, Washington Area*. Retrieved April 13, 2019, from https://www.researchgate.net/profile/Lisl_Zach/publication/268361197_Microblogging_for_Crisis_Communication_Examination_of_Twitter_Use_in_Response_to_a_2009_Violent_Crisis_in_the_Seattle Tacoma_Washington_Area/links/551a8b680cf244e9a4588838/Microbloggin-for-Crisis-Communication-Examination-of-Twitter-Use-in-Response-to-a 2009 Violent-Crisis-in-the-Seattle-Tacoma-Washington-Area.pdf

Identity Theft Resource Center. (2014). Identity theft resource center breach reports. Retrieved December 8, 2018, from https://www.idtheftcenter.org/images/ breach/DataBreachReports_2014.pdf

Jin, Y. (2010). Making sense sensibly in crisis communication: How publics' crisis appraisals influence their negative emotions, coping strategy preferences, and crisis response acceptance. *Communication Research, 37*(4), 522-552. doi: 10.1177/0093650210368256

Jin, Y., & Liu, B. F. (2010). The Blog-Mediated Crisis Communication Model: Recommendations for Responding to Influential External Blogs. *Journal of Public Relations Research, 22*(4), 429-455. doi:10.1080/10627261003801420

Ketchen, D. J., Adams, G. L., & Shook, C. L. (2008). Understanding and managing CEO celebrity. *Business Horizons, 51*(6), 529-534. doi:10.1016/j.bushor.2008.06.003

Kiambi, D.M. & Shafer, A. (2015). Corporate Crisis Communication: Examining the Interplay of Reputation and Crisis Response Strategies, *Mass Communication and Society*, 19(2), 127-148. doi: 10.1080/15205436.2015.1066013

Kim, B., Johnson, K. J., & Park, S. Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management***,** *4*(1). Retrieved December 8, 2018, from https://doi.org/10.1080/23311975.2017.1354525.

Klein, J., & Dawar, N. (2004). Corporate social responsibility and consumers attributions and brand evaluations in a product–harm crisis. *International Journal of Research in Marketing, 21*(3), 203-217. doi:10.1016/j.ijresmar.2003.12.003

Knapp, M. L., & Daly, J. A. (2002). *Handbook of interpersonal communication.* Thousand Oaks, CA: SAGE Publications.

Lariscy, R. A., Avery, E. J., Sweetser, K. D., & Howes, P. (2009). An examination of the role of online social media in journalists' source mix. *Public Relations Review, 35*(3), 314-316. doi: 10.1016/j.pubrev.2009.05.008

Leung, L., & Lee, P. S. (2005). Multiple determinants of life quality: The roles of Internet activities, use of new media, social support, and leisure activities. *Telematics and Informatics, 22*(3), 161-180. doi:10.1016/j.tele.2004.04.003

Lyon, L., & Cameron, G. T. (2004). A Relational Approach Examining the Interplay of Prior Reputation and Immediate Response to a Crisis. *Journal of Public Relations Research, 16*(3), 213-241. doi:10.1207/s1532754xjprr1603_1

Martinko, M. J., Douglas, S. C., Ford, R. C., & Gundlach, M. J. (2004). Dues Paying: A Theoretical Explication and Conceptual Model. *Journal of Management, 30*(1), 49-69. doi:10.1016/j.jm.2002.12.002

Matthews, B. & Ross, L. (2010). *Research methods: A practical guide for the social sciences.* Harlow: Longman.

McDonald, L., A.I. Glendon, and B. Sparks. (2011). Measuring consumers' emotional reactions to company crises: Scale development and implications. *Advances in Consumer Research, 39*. 333–340. Retrieved January 17, 2019, from http://www.acrwebsite.org/volumes/v39/acr_v39_9627.pdf.

Möhring, W. & Schlütz, D. (2010). *Die Befragung in der Medien- und Kommunikations- wissenschaft: Eine praxisorientierte Einführung* (2nd edition). Wiesbaden: Springer VS.

Neuman, W.L. (2014). Survey Research. In W.L. Neuman (Ed.), *Social Research Methods: Qualitative and Quantitative Approaches* (7th edition). Pearson.

North, A. C., Desborough, L., & Skarstein, L. (2005). Musical preference, deviance, and attitudes towards music celebrities. *Personality and Individual Differences, 38*(8), 1903-1914. doi:10.1016/j.paid.2004.11.016

Pallant, J. (2007). SPSS Survival Manual. McGraw-Hill: Open University Press.

Pew Internet & American Life Project. (2006). Blogger callback survey. Retrieved from http://www.pewinternet.org

Ponzi, L. J., Fombrun, C. J., & Gardberg, N. A. (2011). RepTrak™ Pulse: Conceptualizing and Validating a Short-Form Measure of Corporate Reputation. *Corporate Reputation Review, 14*(1), 15-35. doi:10.1057/crr.2011.5

Porritt , D . (2005). The reputational failure of financial success: The ' bottom line backlash effect'. *Corporate Reputation Review, 8*(3), 198–213 . doi: 10.1057/palgrave.crr.1540250

PRC (Privacy Rights Clearinghouse). (2017). Data breaches. Retrieved from https://www.privacyrights.org/databreaches

Punch, K. F. (2014). *Introduction to social research: Quantitative and qualitative approaches* (3rd edition). Sage.

Ramakrishna, A. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, *8*, 33–56. doi: 10.1080/15536548.2012.10845654

Reidenbach, R. E., & Pitts, R. E. (1986). Not all CEOs are Created Equal as Advertising Spokespersons: Evaluating the Effective CEO Spokesperson. *Journal of Advertising, 15*(1), 30-46. doi:10.1080/00913367.1986.10672986

Rhee, M., & Haunschild, P. R. (2003). The Liability Of Good Reputation: A Study Of Product Recalls In The U.S. Automobile Industry. *Organization Science*, *17*(1), 101-117. doi: 10.1287/orsc. 1050.0175

Rice, S., Winter, S. R., Doherty, S., & Milner, M. (2017). Advantages and Disadvantages of Using Internet-Based Survey Methods in Aviation-Related Research. *Journal of Aviation Technology and Engineering, 7*(1), 58-65. doi:10.7771/2159 6670.1160

Roberts, P. W., & Dowling, G. R. (2002). Corporate reputation and sustained superior financial performance. *Strategic Management Journal, 23*(12), 1077-1093. doi:10.1002/smj.274

Salkind, N. J. (2010). *Encyclopedia of research design*. Los Angeles: SAGE.

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2017). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising, 37*(4), 650-663. doi:10.1080/02650487.2017.1348329

Schultz, F., Utz, S., & Göritz, 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. doi:10.1016/j.pubrev.2010.12.001

Seeger, M. W., & Ulmer, R. R. (2001). Virtuous Responses to Organizational Crisis: Aaron Feuerstein and Milt Cole. *Journal of Business Ethics, 31*, 369-376.

Retrieved April 13, 2019, from https://link.springer.com/content/pdf/10.1023/A:1010759319845.pdf.

Sheldon, C. A., & Sallot, L. M. (2008). Image Repair in Politics: Testing Effects of Communication Strategy and Performance History in a Faux Pas. *Journal of Public Relations Research, 21*(1), 25-50. doi:10.1080/10627260802520496

Sohn, D. (2009). Disentangling the Effects of Social Network Density on Electronic Word-of-Mouth (eWom) Intention. *Journal of Computer – Mediated Communication, 14*(2), 352-367. doi:10.1111/j.1083-6101.2009.01444.x

Statista. (2019a). Number of monthly active Facebook users worldwide as of 3rd quarter 2018 (in millions). Retrieved January 15, 2019, from https://www.statista.com/statistics/264810/number-of-monthly-active facebook-users-worldwide/

Statista. (2019b). Most popular social networks worldwide as of January 2019, ranked by number of active users (in millions). Retrieved February 7, 2019, from https://www.statista.com/statistics/272014/global-social-networks-ranked-by number-of-users/

Treadway, D. C., Adams, G. L., Ranft, A. L., & Ferris, G. R. (2009). A meso-level conceptualization of CEO celebrity effectiveness. *The Leadership Quarterly, 20*(4), 554-570. doi:10.1016/j.leaqua.2009.04.008

Turk, J. V., Jin, Y., Stewart, S., Kim, J., & Hipple, J. (2012). Examining the interplay of an organizations prior reputation, CEOs visibility, and immediate response to a crisis. *Public Relations Review, 38*(4), 574-583. doi:10.1016/j.pubrev.2012.06.012

Van Riel, C. B. M., & Fombrun, C. J. (2007). Essentials of corporate communication: Implementing practices for effective reputation management. New York: Routledge.

Veltsos, J. R. (2012). An Analysis of Data Breach Notifications as Negative News. *Business Communication Quarterly*, *75*(2), 192-207. doi:10.1177/1080569912443081

Vidmar, N. (1993). Empirical Evidence on the Deep Pockets Hypothesis: Jury Awards for Pain and Suffering in Medical Malpractice Cases. *Duke Law Journal, 43*(2), 217-266. Retrieved 20 December, 2018, from http://dx.doi.org/10.2307/1372792

Wang, P., & Park, S. A. (2017). COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING. *Issues in Information Systems, 18*(2), 136-147. Retrieved December 21, 2018, from http://www.iacis.org/iis/2017/2_iis_2017_136-147.pdf

Wang, Y., & Wanjek, L. (2018). How to Fix a Lie? The Formation of Volkswagen's Post-crisis Reputation Among the German Public. *Corporate Reputation Review, 21*(2), 84-100. doi:10.1057/s41299-018-0045-8

Ward, J. C., & Ostrom, A. L. (2006). Complaining to the Masses: The Role of Protest Framing in Customer-Created Complaint Web Sites. *Journal of Consumer Research, 33*(2), 220-230. doi:10.1086/506303

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

Weiner, B. (1972). Attribution Theory, Achievement Motivation, and the Educational Process. *Review of Educational Research*, *42*(2), 203-214. doi: 10.2307/1170017

Weiner, B. (2010). *Social motivation, justice, and the moral emotions: An attributional approach*. New York: Psychology Press.

Wigley, S., & Fontenot, M. (2010). Crisis managers losing control of the message: A pilot study of the Virginia Tech shooting. *Public Relations Review, 36*(2), 187 189. doi:10.1016/j.pubrev.2010.01.003

Wright, D., & Hinson, M. D. (2009). An Updated Look at the Impact of Social Media on Public Relations Practice. *Public Relations Journal*, *3*(2). Retrieved April 13, 2019, from https://prjournal.instituteforpr.org/wp-content/uploads/An Updated-Look.pdf.

Zhou, S. & Sloan, WM.D. (2011). *Research Methods in Communication* (2nd. edition). Northport: Vision V Press.

## 9. Appendices

***Appendix A***: Questionnaire

**Introduction for participants**

Welcome to our survey and thank you for participating. The survey is part of a research Master thesis project at Erasmus University. We would like you to fill out all the questions in the questionnaire after reading the news article; please read and answer all the questions carefully. This questionnaire will take approximately 10 minutes. Moreover, all information gathered from this survey will be confidential and the data will only be used for the purpose of this research. Your participation in this experiment is totally voluntary.

1.What is your age?

2.What is your gender?

- Male
- Female
- Other

3.What is your nationality?

4.What is your highest education level?

- Below High School
- High School
- College study (equivalent to Applied Science)
- University (Bachelor's Degree)
- Master's Degree
- Doctorate

5.Did you ever have a Facebook account?

- Yes
- No

6.How many years have you been using Facebook?

- Less than a year
- 1-3 years
- 4-6 years
- 7-9 years
- 10 years or more

7.How often do you use Facebook per day?

- Less than once per day
- 1-3 times per day
- 4-6 times per day
- 7-9 times per day
- More than 10 times per day

8.Please indicate how much you agree or disagree with the following statements

- I have a good feeling about Facebook
- I trust Facebook
- I admire Facebook
- Facebook has a good overall reputation

9.Do you know Mark Zuckerberg, the CEO of Facebook?

- Yes*
- No

*if Yes:

9a.Please indicate how much you agree or disagree with how clearly the phrase represents your view of the CEO of Facebook (Mark Zuckerberg)

- I have a good feeling about him
- I admire and respect him
- He has some characteristics I would want to have

- I like to learn more about him

10.Below there is an article explaining the Facebook - Cambridge Analytica scandal

The New York Times

## *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*

By Kevin Granville

Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to private information on more than 50 million Facebook users. The firm offered tools that could identify the personalities of American voters and influence their behavior.

The data, a portion of which was viewed by The New York Times, included details on users' identities, friend networks and "likes." The idea was to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with digital ads.

11.Have you heard about this scandal before?

- Yes
- No

12.Please indicate how much you agree or disagree with the following statements:

- The Facebook – Cambridge Analytica scandal was an intentional act by someone in the organization
- Someone in the organization knowingly created Facebook – Cambridge Analytica scandal
- The organization had the capability to stop the Facebook – Cambridge Analytica scandal from occurring
- The Facebook – Cambridge Analytica scandal was preventable by the organization
- The organization could have avoided the Facebook – Cambridge Analytica scandal

- The organization should be held accountable for the Facebook – Cambridge Analytica scandal
- The Facebook – Cambridge Analytica scandal was caused by a weakness in the organization
- Internal organizational issues contributed to the Facebook – Cambridge Analytica scandal

13.After the Facebook - Cambridge Analytica Scandal how likely are you going to do the following?

- I am likely to share the message with other people (show/forward/retweet).
- I am likely to tell my friends about the incident.
- I am likely to leave a comment against Facebook on social media.

14.Please indicate how much you agree or disagree with the following statements'

- Regarding the Facebook – Cambridge Analytica scandal, Facebook is concerned with the well-being of its publics (e.g., customers, employees, investors)
- Facebook is basically dishonest concerning the emissions scandal
- I do not trust Facebook to tell the truth about the emissions scandal
- Under most circumstances, I would be likely to believe what the Facebook says about the emissions scandal
- Regarding the Facebook – Cambridge Analytica scandal, Facebook is not concerned with the well-being of its publics (e.g., customers, employees, investors)

END.

Thank you for your time and for filling out the questionnaire.