Data Breach Crisis

The impact of crisis type, pre-crisis reputation, and crisis response strategy on perception on organizations

Student Name: Charlotte Vollebregt
Student Number: 531989

Supervisor: Dr. Yijing Wang

Master of Media Studies - Media & Business
Erasmus School of History, Culture, and Communication
Erasmus University Rotterdam

Master's Thesis Media & Business
June 2020

DATA BREACH CRISIS: THE IMPACT OF CRISIS TYPE, PRE-CRISIS REPUTATION, AND CRISIS RESPONSE STRATEGY ON PERCEPTION ON ORGANIZATIONS

ABSTRACT

Due to the rise of the Internet, the automatic collection of information of online users and transformation into extensive data collections keeps on expanding. The threat for online users is that these data gathering practices of organizations could result in the occurrence of a data breach crisis. For organizations situated in a data breach crisis, it is challenging to manage stakeholders' perceptions and engagement in secondary crisis communications. The issue of data breach crisis is a relatively new topic, which makes it relevant to explore this with an audience-centered focus since little research has been done on this context. This study was conducted using three data breach crisis types (intentional and internal crisis vs. unintentional and internal crisis vs. intentional and external crisis), two crisis response strategies (denial vs. no response) and a different pre-crisis reputation (high vs. low). These factors, in combination with two stakeholder emotions, namely anger and sympathy, and individual privacy concerns, were connected to the perception on organizations. Also, emotion and individual privacy concerns were connected to secondary crisis communication. In this way, the results of this study provide a broad understanding of which factors are essential for organizations to keep in mind to control stakeholders' perceptions and the resulting secondary crisis communications. The following research questions were conducted: "How do crisis type (intentional and internal vs. unintentional and internal vs. intentional and external), crisis response strategy (denial vs. no response) and pre-crisis reputation (high vs. low) affect the perception on organizations after a data breach crisis?" and "What are the roles of emotion and individual privacy concerns on the perception on organizations and secondary crisis communication?". An experiment design was developed by using the online tool 'Qualtrics' to answer the research questions. The online experiment was implemented by using a 3 X 2 X 2 factorial between-subject design for a total of twelve

conditions. A convenience sampling method was distributed by using the online tool ‘Amazon Mechanical Turk’. After cleaning the data, 563 participants were included in the final dataset. The results showed a significant impact of the difference of an intentional and internal data breach crisis and an intentional and external data breach crisis, the difference between high and low pre-crisis reputation, and intensity of emotion on the perception on organizations. Also, the intensity of emotion and individual privacy concerns had a significant impact on secondary crisis communication. When an organization has to deal with managing a data breach crisis, the results indicate that the most important aspects to keep in mind are the internal or external occurrence of the crisis, the reputation of the organization before the crisis, stakeholders’ emotions towards the organization, and individual privacy concerns. More extensive research on this field is required for both marketers and scholars to develop a deeper understanding of the impact of data breach crisis on stakeholders.

KEYWORDS: data breach crisis, crisis response strategy, pre-crisis reputation, privacy concern, secondary crisis communication

Table of Contents

1. Introduction

The invention of the Internet assisted the evolution of human knowledge as a whole (Berners-Lee, Hendler & Lassila, 2001). However, the understanding of the developments on the Internet is getting more complicated due to all the processes that run in the background that only few online users are aware of (Barth, de Jong, Junger, Hartel & Roppelt, 2019). In 2001, the term Semantic Web was used for the first time by Berners-Lee et al, which indicates that the web consists of data that can be controlled by machines. Until now, the Internet collects information from its online users and transforms this information into an extensive data collection that can be processed automatically and keeps on expanding (Berners-Lee et al., 2001). These data gathering practices are increasing in volume and detail, due to the rise of social media, the Internet of Things (IoT), and multimedia, which leads to an overwhelming flow of data (Hashem, Yaqoob, Anuar, Mokhtar, Gani & Khan, 2015). On the one hand, this Big Data collection can be seen as an opportunity for Internet users. These users have access to tons of information, which results in the trigger of innovation, communication, and freedom of expression (Cumbley & Church, 2013). On the other hand, the threat of Big Data for Internet users is that these new data pools can have the consequence that their personal information can be exposed, which results in privacy breaches on a high level (Cumbley & Church, 2013). Such breach incidents can be seen as forms of organizational crises, which are described as specific, unexpected, and non-routine events that could threaten the organization's reputation and goals (Schultz, Utz & Goritz, 2011). In this digital era, where online sharing is a prevalent occupation due to social media, users are authorized to create, find and share information about organizations situated in a crisis in the form of secondary crisis communications which shapes these crises as more numerous, destructive and apparent with more additional effects and casualties (Mangold & Faulds, 2009; Seeger, Sellnow & Ulmer, 2003).

Data breaches are noticeable as violations that endanger sensitive, protected, or confidential data of Internet users (Zou, Danino, Sun & Schaub, 2019). The issue of data breaches is relatively contemporary and has not been investigated regularly, even though this phenomenon is becoming more common nowadays and has specific effects

on consumers. To clarify, the pattern of today's data abuse can be explained by considering the first half of 2019, where more than 3.800 publicly disclosed breaches have been discovered, exposing 4.1 billion compromised records (Winder, 2019).

An organization that uses the Internet to collect information from its online users to create a comprehensive data collection is the American multinational technology company Google. Google's privacy policy allows information from its search engine, YouTube usage, and mapping service to be used to help the company to build a more detailed profile of its users, which increases the effectiveness of its advertisements. In this way, Google explicitly knows what its consumers want to know, what they are watching, and where they live (Cumbley & Church, 2013). The Google+ data leak scandal of 2018 is a well-known example of how a data breach crisis can influence the perceptions of stakeholders. Google reached the newspapers with a scandal in which third-party app developers could access the data of, not only the users of the Google+ platform, but also of their friends. Google decided not to disclose the user data leak, occurring from a bug in the API for Google+ in March 2018. The reason for the non-disclosure of the news was because the company wanted to avoid damage to public relations and potential regulatory enforcement (Wong & Solon, 2018). This data leak affected up to 500.000 Google+ accounts. Besides, up to 438 different third-party applications had access to private information due to the bug. When this story came in the news, a lot of controversial perceptions on the crisis came up. Some people thought it was Google's right to not disclose about the crisis, although others considered that the data breach crisis was further evidence that large technology platforms need more regulatory oversight. In the end, Google decided to shut down consumer access to Google+ and to improve its privacy protections for third-party applications (Wong & Solon, 2018). In this situation, an organization with a high reputation situated itself in an unintentional and internal data breach crisis and decided not to respond to the situation, which evolved some different perceptions and secondary crisis communications from stakeholders. To learn from an example like this, an organization should understand how to protect its reputation and which response strategy is best to use in different kinds of data breach situations. Therefore, it could be stated that it is essential to respond effectively to different types of data breach crisis since the relevance of various

corporate reputation dimensions from a stakeholders' perspective vary dependending on each type of data breach crisis (Confente, Siciliano, Gaudenzi & Eickhoff, 2019). To make it more practical, managing in the most efficient way and establishing the most suitable communication strategy towards stakeholders requires crisis managers to distinguish which data breach type their company is facing (Confente et al., 2019). An organization's poor behavior after a data breach crisis can damage the trust of the organization's stakeholders, making the organization suffer from a loss in corporate reputation (Davies & Olmedo-Cifuentes, 2016). In this way, it becomes clear that it is more important than ever for organizations to manage their corporate reputations in this globalizing digital world. This research will assess the impact of a data breach crisis, pre-crisis reputation, and crisis response strategies on perceptions among the public. Also, different emotions and individual privacy concerns are included in this study, focussing on perceptions on organizations and secondary crisis communication intentions. This research tries to address this issue by implementing an experimental design using fictitious newspaper articles.

To specify, one of the elements that can influence the perception on organizations is the type of data breach crisis. These data breach crises can be classified into three categories: an intentional and internal data breach crisis, an unintentional and internal data breach crisis, and an intentional and external data breach crisis (Confente et al., 2019). Recent literature focuses more on a single data breach crisis, which means that broader investigation is essential to recognize if perceptions of the damage are affected differently according to different types of data breach crisis (Confente et al., 2019).

From the perspective of the organization, it is interesting to differentiate what kind of response strategy works best to handle the situation of a crisis. To help these organizations, the Situational Crisis Communication Theory was developed as a general guide, which will also support this research (Coombs, 2007). The SCCT model explains that different forms of crises require different crisis response strategies eventually leading to different public's perceptions on this crisis and organization (Coombs, 2007). When a crisis response strategy is managed well, organizations can minimize their reputation to be injured. A denial response strategy is, when believed by its

stakeholders, a way to reduce reputational harm for an organization (Coombs, 2007). In contrast, giving no response at all creates the most reputational damage to an organization (Coombs, 2006). Therefore, this research investigates the effects of two different response strategies, namely denial and no response, to perceive the most appropriate strategy in different data breach situations.

Moreover, another element included in this study that can influence the perception on organizations during a data breach crisis is pre-crisis reputation. A reputation of an organization can be seen as the perception of stakeholders on how well an organization meets the expectations based on previous performances (Coombs, 2007). Pre-crisis reputation can be linked to reputational capital. This capital works as a buffer, which means that companies with a favorable pre-crisis reputation can deal with more reputational damage than companies with an unfavorable or neutral pre-crisis reputation (Coombs, 2007). The rise of digitalization brings both advantages and disadvantages for corporate reputations. When a reputation is positive, it can lead to many useful contributions, but the digital landscape also challenges companies to have a grip on their reputation (Dijkmans, Kerkhof & Beukeboom, 2015). Also, the role of stakeholders is changing since they can voice their perceptions through the use of social media. Consumers no longer play the role of passive receivers, which was the case in classic crisis and reputation communication practices. It can, therefore, be stated that corporate reputation is essential to control stakeholders' perceptions (Zheng, Liu & Davison, 2018).

According to these findings in the literature, this research will continue to investigate the combination of the concepts of data breach crisis, crisis response strategy, pre-crisis reputation, emotion, and individual privacy concern. In this way, this research will contribute to the academic field of crisis communication by exposing the effects of different variables on the perception on organizations occurring in a data breach crisis. Also, the effect of emotion and individual privacy concerns on secondary crisis communication will be included. Therefore, by applying an experimental research design, the following research questions are stated:

***RQ1**: How do crisis type (intentional and internal vs. unintentional and internal vs. intentional and external), crisis response strategy (denial vs. no response), and pre-crisis reputation (high vs. low) affect the perception on organizations after a data breach crisis?*

***RQ2:** What are the roles of emotion and individual privacy concerns on the perception on organizations and secondary crisis communication?*

1.1 Social and scientific relevance

This study contributes to the academic field of crisis communication by investigating the effects of different indicators that could explain stakeholders' perception on organizations situated in a data breach crisis and stakeholder's secondary crisis communications. The subject of crisis communication has been approached from different academic perspectives, but limited in-depth research has been done towards the perceptions on different types of data breaches crises since this is a relatively new phenomenon. Moreover, most crisis communication research concentrates on finding effective response strategies for companies but neglects the investigation of the processes that generate a more natural understanding of the public's reactions to organizations in crisis (Kim, 2019). It is necessary to develop an audience-centered focus to interpret how different factors influence perceptions on and reactions to data breach crises, which can lead to information for crisis managers informing them how the public is likely to respond. In that way, crisis managers can arrange their crisis responses properly (Coombs & Holladay, 2011).

The social relevance of studying data breaches can be explained by mentioning that in today's society, in which data breach crises play an increasing vital role, companies need to take another look at their traditional crisis communication strategies and try to adapt them to the new challenges these kinds of new forms of crises provide. These data breach crises can be seen as a relatively new kind of problem related to privacy issues, in which these privacy issues are a primary concern that has increased in the last few years (Alemany, del Val, Alberola & García-Fornes, 2019). When stakeholders are aware of organizational data-gathering practices and its

consequences, individual perceptions will rise, which are relevant for investigation. Also, cybersecurity plays a vital role in the development of information technology and services. This is because cyber-attacks have become a big issue in the digital economy (Das & Patel, 2017). Cyber-attacks can eventually lead to substantial data breach crises for businesses that require well-organized crisis management to minimize the damage to their business reputation (Wang & Park, 2017). For example, according to Maal and Wilson-North, one of the do's of social media as a first communication point during a crisis by any organization is to be honest and transparent when posting information (2019). In this way, an organization is minimizing additional threats after a crisis and keeps a positive relationship with its customers to prevent them turning to other sources (Veil, Buehner & Palenchar, 2011). To conclude, the societal relevance of this study is pointed at the increasing number of corporate crises that are stated as a data breach crisis. For organizations, the rise of the Internet increases the awareness that the public can become the final judge when it comes to organizations' behavior. Therefore, it is relevant to determine which factors affect the public's perspective and communications after a data breach crisis to increase the knowledge of crisis communication.

2. Theoretical Framework

2.1 Corporate crisis and crisis communication

A corporate crisis can be a risk for the market position of an organization since it damages the organizational reputation which can eventually affect how stakeholders (e.g., community members, employees, customers, suppliers, and stockholders) relate to an organization (Coombs & Holladay, 2006; Coombs, 2007). A crisis is defined as “a sudden and unexpected event that threatens to disrupt an organization’s operations and poses both a financial and a reputational threat” (Coombs, 2007, p. 164). To conceptualize theories about and how to manage crises, the Situational Crisis Communication Theory (SCCT) developed by Coombs is one of the cornerstones of the crisis communication academic field (2007). This theory develops a framework for understanding how people interpret a crisis by assessing the level of reputational threat, depending on attribution, crisis history, and prior relationship. It also describes how to use post-crisis communication to maximize the protection of organizational reputation and minimize unfavorable secondary crisis communications (Coombs, 2007; Kim, 2019).

SCCT has its roots lie in the Attribution Theory which concludes that people look for causation after occurring events, especially those that are negative and unexpected (Coombs, 2007; Weiner, 1985, 1986, 2006). For example, when a particular public event is canceled due to the Corona Crisis, ticket holders will connect little blame attributions to the organization board of the event because the virus can be seen as unpredictable, called a black swan. These kinds of situations go beyond what is usually expected and have serious consequences (Hajikazemi, Ekambaram, Andersen & Zidane, 2016). Consequently, after the occurrence of a crisis situation, stakeholders will get an emotional reaction. In the Attribution Theory, there are two core emotions: anger and sympathy. When stakeholders have high attributions towards the crisis responsibility of an organization, this may result in more anger, although low attributions towards the crisis responsibility of an organization result in more sympathy (Coombs, 2007). Therefore, it is essential as an organization to be aware of stakeholder

attributions since the responsibility of a crisis can lead to dissatisfaction and negative word of mouth.

Another theory the SCCT is based on is the Image Restoration Theory, which explains the power of communication of an organization after a crisis to protect its reputation against adverse reactions to a crisis (Benoit, 1995; Coombs, 2007). The SCCT model extends this Image Restoration Theory by presenting a system that predicts which communication strategies are the best solutions after deciding how stakeholders should react to the crisis. Managers try to anticipate this by using crisis response strategies to protect the reputation of their organization by either denying, diminishing, or rebuilding the crisis (Coombs, 2007). These crisis response strategies will be discussed more broadly later in this research.

To evaluate the reputational threat of a crisis using SCCT, crisis managers first determine the primary crisis responsibility attached to a crisis which depends on each framed crisis type. The more stakeholders attribute towards an organization, the lower the reputational score of that organization (Coombs, 2007). Based upon the attributions of crisis responsibility, the SCCT defines three clusters: (1) the victim cluster has very powerless attributions of crisis responsibility because the organization is seen as victim of the crisis; (2) the accidental cluster has slightest attributions of crisis responsibility, because the organization is not able to control the crisis and (3) the intentional cluster has very powerful attributions of crisis responsibility, because the crisis happened intentionally (Coombs, 2007; Coombs & Holladay, 2002). For this study, the focus will lie on three different data breach crises that can be assigned to all three of these clusters to collect information on the different outcomes of these clusters on the perception on organizations.

The second step for crisis managers is to determine additional factors, namely crisis history and prior relationship reputation, which are both based on past situations. Crisis history means if an organization has experienced a similar crisis in the past. Besides, prior relationship reputation means how an organization behaved to its stakeholders in the past. These concepts mean that an organization suffers from more reputational damage, if it had an experience with a similar crisis some years ago or if it treated stakeholders unfavorably before (Coombs, 2007). An adverse crisis history or

relationship can make stakeholders less forgiving because they already have a negative image of the organization, and the crisis can furthermore strengthen this assumption (Coombs, 2004; 2007). At the same time, a favorable crisis history or relationship is built by meeting stakeholders' expectations in the past. This results in the ignorance of stakeholders of negativities of a crisis and the perception on the crisis as a rare misstep (Coombs & Holladay, 2001).

When the responsibility of a crisis is low and crisis history and prior relational reputation are favorable, there is a reduction of the damage of an organizational crisis. However, when the responsibility of a crisis is high and crisis history and prior relational reputation are unfavorable, they can create a situation where the organizational crisis will increase and lead to more reputational damage (Coombs, 2007). As demonstrated, every crisis is a collection of different circumstantial considerations, behaviors, and outcomes, which makes it very difficult to decide on a 'best practice' for crisis communication. Assuming uniformity is, therefore, not possible, and every crisis should be treated individually (Coombs, 2015).

Most previous studies using the SCCT model are concentrated on finding the most effective corresponding response strategies or examining case studies focusing on real-used response strategies related to the classification of different crisis types (Coombs, 2004; Coombs & Holladay, 2002; Kim, 2019). These different crisis types and response strategies, combined with the attribution of emotion, pre-crisis reputation, and privacy concern, will be a crucial contribution to this research and will, therefore, be discussed subsequently below.

2.2 Privacy issues and data breach crisis

The emergence of the Semantic Web has brought up large scale data collections, which raised severe privacy and security issues (Barth & de Jong, 2017). Companies gather personal data in the background of general Internet, e-commerce, social networking, and mobile application activities since they want to create a more knowledgeable image of their customer base. In that way, they can target the right groups of potential customers with the right products or services (Flender & Müller, 2012). This process often happens without online users knowing. These online

performances conducted by companies may mean a breach of online user's privacy on the Internet.

On the one hand, in our modern information society, online users have an interest in keeping their privacy safe and maintain a positive attitude towards privacy-protecting behavior. However, on the other hand, they release their data in full disclosure and are therefore not acting protective at all (Pötzsch, 2008). This circumstance can be explained by the fact that users are inclined to online privacy-compromising behavior, which leads to a contrast between privacy attitudes and actual behavior (Acquisti & Grossklags, 2005). This contradiction is what many researchers call the privacy paradox: online users assure they are concerned about their privacy but do not behave in a way they want to protect their data (Pötzsch, 2008). Retail value and personalized services seem to be more important than the awareness of privacy risks (Acquisti & Grossklags, 2005). The first study that came up with the privacy paradox, written by Brown, can be seen as a landmark study of this concept (2001). Brown investigated online shoppers and discovered through in-depth interviewing that the participants of this research group were willing to disclose their personal information if they had something to gain in return, conforming to their purchased products. After this first study, many theories are written by researchers to explain the privacy paradox, supporting or rejecting the concept. However, there is still no one-sided accepted theory that explains online behaviors and mental processes of users when deciding whether to disclose information or not (Barth & de Jong, 2017).

The awareness of privacy issues raised because of the appearance of data breaches, which can be categorized into different types to understand the various effects of those breaches and the different strategies helping crisis managers to control the crises (Confente et al., 2019; Coombs, 2007). This differentiation of crisis type can be explained in the way of how a crisis is being framed, which operates on two related levels: frames in communication and frames in thought. Frames in communication are words, phrases, and images that present information in a message, like a newspaper article. In thought, frames are cognitive structures that people use when they translate information (Coombs, 2007; Druckman, 2001). Frames in communication decide how people will shape their frames in thought, how they define problems, causes of

problems, attributions of responsibility, and solutions to problems (Coombs, 2007; Cooper, 2002). Crisis types can also be seen as a structure of a frame since its indications decide on how stakeholders will react to a crisis (Coombs & Holloday, 2002). The indications of a crisis type could be whether the crisis happened due to an internal or external enforcement or whether the crisis occurred intentionally or unintentionally. These factors decide how much responsibility stakeholders will assign to a crisis incident (Confente et al., 2019; Coombs, 2007).

As has been said before, crisis types can be divided into three clusters based on crisis responsibility (Coombs, 2007). Data breach crises can be linked to these clusters based on internal/external and intentional/unintentional indicators. The first data breach category is called intentional and internal, which means that a crisis has been caused intentionally by an internal factor (e.g., vicious employees stealing customers' data). This data breach category can be assigned to the intentional cluster. This cluster has very strong attributions of crisis responsibility and happens purposely (Coombs & Holladay, 2002). The second category is called unintentional and internal, which refers to an accidental crisis event executed by an internal factor (e.g., private information posted publicly due to incorrect security settings). This data breach category can be assigned to the accidental cluster with minimal attributions of crisis responsibility. The last data breach category is called external and intentional, which means that a crisis has been caused intentionally by an external factor (e.g., hacked by an outside party or infected by malware). This data breach category can be assigned to the victim cluster and has very weak attributions of crisis responsibility (Confente et al., 2019; Coombs, 2007). The classification of data breach crises lead to different comments of customers on social media (Confente et al., 2019). Regarding intentional and internal data breaches, the valence is positive concerning user comments since people believe that an organization "should have full control over the management of their employees and should make fast and effective decisions" (Confente et al., 2019, p. 500). Regarding unintentional and internal data breaches, the valence of user comments is in general negative since people feel a negative sense of uncertainty and a lack of commitment from employees (Confente et al., 2019). Finally, regarding intentional and external data

breaches, the valence of user comments is also negative since people have a negative sense of apprehension regarding future consequences (Confente et al., 2019).

Nevertheless, this study focuses on the assumptions connected to the crisis clusters presented in Coomb's SCCT model that affirm that internal crises lead to a higher attribution of crisis responsibility than external crises (2007). Hence, this higher attribution of crisis responsibility leads to a stronger impact on weakening the perception on the organization than an external crisis that generates a lower attribution of crisis responsibility (Coombs, 2007). Also, focusing on these internal data breach crises, the crisis has a stronger impact on weakening the perception on organizations when it has been evolved on purpose instead of accidentally. To clarify, intentional crises generate a higher attribution of crisis responsibility towards the organization than unintentional crises since the intentional crisis is considered purposeful, and the unintentional crisis is considered uncontrollable by the organization (Coombs, 2007).

Based on these arguments, a prediction has been summarized in the following two hypotheses:

H1a: Intentional and internal data breaches have a stronger impact on weakening the perception on organizations compared to unintentional and internal data breaches as well as intentional and external data breaches.

H1b: Unintentional and internal data breaches have a stronger impact on weakening the perception on organizations compared to intentional and external data breaches.

2.3 Crisis response strategy

The SCCT model differentiates various crisis response strategies, which means that there are different ways an organization can communicate during or after a crisis. This communication affects the people's perceptions on this organization and the occurring crisis (Coombs, 2007). After conducting its priority of protecting stakeholders from any damage, some strategies are being used by organizations to reconstruct their reputation, minimize the negativity of a crisis and prevent unwanted attitudes (Coombs, 2007). In the SCCT model, the three different categories of crisis response strategies

are the following: denial, diminish, and rebuild (Coombs, 2007). Denial response strategies guarantee that no crisis has occurred or that the organization has no responsibility. In this way, the organization tries to remove every reputational threat that results after a crisis. Diminish response strategies change the assumptions towards a crisis to make it seem less harmful. The organization tries to make the crisis look less severe about reducing destructive reputational consequences. To finalize, rebuild response strategies try to fix and strengthen reputational valuables. Companies take positive actions in the way of offering apologies or compensation to the victims of a crisis (Coombs, 2007). These three crisis response strategies are based upon perceptions of accepting responsibility for a crisis by an organization.

For this study, the focus will lie on one type of crisis response strategy from the SCCT model, namely the denial strategy. Denial is a way to remove the connection between a crisis and the organization because managers attempt to argue that there is no ‘real’ crisis (Coombs, 2007). This strategy is the most effective in the victim cluster, which means in the intentional and external conditions. In these conditions, there is no evidence of the connection between the organization and the crisis. If stakeholders accept the denial response strategy and believe the organization's argument that there is no crisis, the organization will be saved from any reputational harm. Therefore, in the intentional and external condition, the weakening effects on people’s perception on the organization in crisis are less strong when the organization uses a denial response strategy than a no response strategy (Coombs, 2007).

Focusing on the other two data breach conditions, the SCCT model suggests that in the intentional cluster, thus the intentional and internal condition, rebuild crisis response strategies should be used. Also, the model suggests that in the accidental cluster, thus the unintentional and internal condition, diminish crisis response strategies should be used (Coombs, 2007). Since this study only focuses on denial response strategy and no response strategy, the hypotheses are based on trust violation research that found that the most harmful and ineffective response strategy for organizational reputation, regardless of crisis type, is to give no response at all. This statement can be explained by the fact that stakeholders demand answers, and a no response strategy creates an information vacuum, which may result in speculation, frustration, and loss of

trust among stakeholders (Coombs, 2006; Coombs et al., 2016; Woon & Pang, 2017). Altogether, these above assumptions lead to the following hypotheses:

H2a: Within an intentional and internal crisis, a no response strategy has a stronger impact on weakening the perception on organizations compared to a denial response strategy.

H2b: Within an unintentional and internal crisis, a no response strategy has a stronger impact on weakening the perception on organizations compared to a denial response strategy.

H2c: Within an intentional and external crisis, a no response strategy has a stronger impact on weakening the perception on organizations compared to a denial response strategy.

2.4 Pre-crisis reputation

The construct of corporate reputation can be seen as a multidimensional concept, because different perceptions, expectations and opinions of customers, suppliers, (potential) employees, investors, and local communities decide on this reputation. These different stakeholders' perceptions, expectations, and opinions can be conflicting, which makes the construct of corporate reputation very fragile (Confente et al., 2019). The benefits of a positive reputation for organizations are: attractiveness, trust, credibility, and improved financial gains. These advantages are a reason for companies to maintain such a positive reputation. On the other hand, a negative reputation results in destroying the market position of an organization and creates a situation where stakeholders choose to switch to competitors (Coombs, 2007).

The ever-changing field of this concept becomes more important every year because the time spent on the Internet increases very fast due to digitalization. Social media plays a vital role in people's everyday lives and alters the way consumers and businesses communicate. In this way, managing an organization's reputation on social media becomes more important for the relation with online users (Ott & Theunissen,

2015). It is essential for organizations to communicate as honestly and openly as possible, considering that online users have the aids to discover facts about organizations that they preferred to hide (Ott & Theunissen, 2015). These developments alter the power balance between consumers and organizations, due to the fact of the influence of the increasingly expanded online communication systems that can damage firms' reputations (Becker & Lee, 2019). Easy access to the Internet, open participation, and the fast-spreading abilities of content make it impossible for companies to have supervision about what is being said about them online (Aula, 2010).

Results of the study of Becker and Lee indicate that, despite being aware of the power of the Internet, organizations remain naïve as to how to best communicate with online consumers to control their perceptions and behaviors (2019). This naivety is remarkable, because a favorable pre-crisis reputation of an organization can work as a buffer or ‘reputational capital’, which means that this organization suffers less from specific crises and revives more quickly (Coombs, 2007). Also, organizations with a high pre-crisis reputation will have a higher post-crisis reputation than other organizations that have a lower pre-crisis reputation (Decker, 2012). Stakeholders have a disinclination in changing their attitude towards the pre-crisis reputation of an organization and attribute less responsibility towards that organization. Also, the high pre-crisis reputation of an organization can defend this organization against negativities resulting from newspapers and external complaints after a crisis (Claeys & Cauberghe, 2015).

These phenomena are called the ‘Halo effect’. This effect means the power of a pre-crisis reputation of an organization that blocks negative reputations consequences like a shield (Coombs & Holladay, 2006). Stakeholders will not easily change their own opinions or expectations about an organization due to a crisis because the negativity is prevented by the shield (Coombs & Holladay, 2006). Therefore, it is assumed that in the case of data breaches, a low pre-crisis reputation of an organization will have a stronger impact on weakening people’s perceptions of this organization, because it has no or less reputational capital to block negative effects than an organization with a high pre-crisis reputation. Thereupon, the following hypotheses occur:

H3a: Within an intentional and internal crisis, a low pre-crisis reputation has a stronger impact on weakening the perception on organizations compared to a high pre-crisis reputation.

H3b: Within an unintentional and internal crisis, a low pre-crisis reputation has a stronger impact on weakening the perception on organizations compared to a high pre-crisis reputation.

H3c: Within an intentional and external crisis, a low pre-crisis reputation has a stronger impact on weakening the perception on organizations compared to a high pre-crisis reputation.

2.5 Emotion

Since crises have a substantial chance to become viral due to social media, it can lead to instantly circulating emotions on the Internet. Organizations can be seen as disembodied entities, which makes it easier for them to become targets of negative emotions (Ott & Theunissen, 2015). These negative emotions do have an impact on those organizations, illustrated by Graf and Schwede, in their “shitstorm” social media scale (2012). This scale shows that it is essential to evaluate the emotional impact of a crisis because this alters the reputational risk of this crisis (Graf and Schwede, 2012).

Since crises can harm stakeholders emotionally, the SCCT model also focuses on the importance of negative emotions in different forms of crises (Coombs, 2007). In this model, the Attribution Theory explains that “a person attributes responsibility for an event and will experience an emotional reaction to the event” (Coombs, 2007, p. 165). As mentioned before, the two core emotional reactions in the Attribution Theory are anger and sympathy. When attributions of crisis responsibility increase, the negative emotion of anger will appear, whereas when attributions of crisis responsibility are low, the positive emotion of sympathy will rise (Coombs, 2007; Weiner, 1985). These changes lead to perceptions and behavioral responses like secondary crisis communications of people involved with the crisis. The perceptions on organizations are more unfavorable when anger is evoked and more favorable when sympathy is evoked,

regardless of the crisis type (Coombs, 2007; Weiner, 1985). After the formation of these perceptions, secondary crisis communications are the behavioral actions taken by the stakeholder after a crisis in the way of sharing, commenting, or informing others (Mangold & Faulds, 2009). Anger is being considered to generate intentions for secondary crisis communication since stakeholders are willing to express their feelings about the organization or even their revenge to their close friends, which is less the case with stakeholders who are satisfied with the organization (Coombs, 2007; Wang & Wanjek, 2018). Although, a high level of sympathy results in stakeholders' willingness to use secondary crisis communications to support the organization (Wang & Wanjek, 2018). Regarding these arguments, the following hypotheses are presented:

H4a: When there is a data breach crisis, more anger towards an organization has a stronger impact on weakening the perception on organizations compared to less anger.

H4b: When there is a data breach crisis, more sympathy towards an organization has a stronger impact on strengthening the perception on organizations compared to less sympathy.

H4c: When there is a data breach crisis, more anger towards an organization has a stronger impact on secondary crisis communication compared to less anger.

H4d: When there is a data breach crisis, more sympathy towards an organization has a stronger impact on secondary crisis communication compared to less sympathy.

2.6 Privacy concern

General privacy concerns explain the consumer's beliefs, attitudes, and perceptions towards privacy issues like the collection of personal information, the user's control over the collected information and the user's awareness of how the collected information is used, which can all depend on individual privacy traits or personality differences (Malhotra, Kim & Agarwal, 2004; Motiwalla, Li & Liu, 2014). Moreover, privacy concern is a construct to measure an individual's discomfort towards the privacy

practices of an organization (Dinev & Hart, 2006). After the occurrence of some online privacy scandals, it is evident that people are more aware of the relevance of privacy and are giving more attention to personal information disclosure on the Internet (Yu, Li, He, Wang and Jiao, 2020). On the one hand, some studies agree that privacy concerns can reduce the disclosure of personal information of Internet users (Bansal, Zahedi & Gefen, 2010; Wang, Duong & Chen, 2016). On the other hand, studies conclude that the disclosure of personal information is not consistent with privacy concerns that relate to the privacy paradox (Acquisti & Grossklags, 2005; Pötzsch, 2008). Despite the conflicting academic results in this context, it can be stated that privacy concern is an essential concept in the field of Internet privacy and plays an essential role in the privacy decision making process of online users (Smith, Dinev & Xu, 2011; Yu, et al., 2020).

Regarding this privacy concern, individuals can be divided into three different categories based on the Westin-Harris consumer privacy surveys conducted between the late 1970s until 2004. These Westin-Harris privacy indexes are benchmarks of general consumers' privacy concerns and attitudes, valued by thousands of US consumers and validated by other privacy concern studies. Individuals are divided into three categories known as: privacy fundamentalist, privacy pragmatist, and privacy unconcerned (Harris & Westin,1991; Motiwalla et al., 2014). To explain, privacy fundamentalists are very uncomfortable with how online institutions deal with their online information, and perceive this phenomenon as a threat to their privacy. Therefore, they have trust issues towards organizations when sharing their data (Motiwalla et al., 2014). Then, privacy pragmatists are somewhat uncomfortable with the manner of how online institutions deal with their online information, so they weigh the risks of releasing personal information against the potential benefits, like personalization or rewards (Motiwalla et al., 2014). To finalize, privacy unconcerned people are very comfortable with sharing personal information and think the opposite of the fundamentalists. They think that there is no problem with how online institutions deal with their online information, and they perceive this phenomenon as no threat to their privacy (Motiwalla et al., 2014). Privacy concern is often related to the privacy paradox, meaning that Internet users generally think about the protection of their privacy as an

important factor, even though they do not let this concern affect their online self-disclosing behavior (Taddicken, 2014).

Nonetheless, a few assumptions can be made looking at the different categories of a general privacy concern regarding the extent to which individuals are more sensitive to privacy traits. Privacy fundamentalists have trust issues towards organizations, privacy pragmatists vary on perceptions depending on the situation, and privacy unconcerned do not feel threatened at all. This is why privacy concern is considered a negative tendency, and it can be stated that the higher individual concern, the stronger the impact on weakening the perception on organizations regardless of the type of data breach crisis. This assumption is in line with the above-spoken subject about emotions, in which it is stated that anger also results in a stronger impact on weakening the perception on organizations and a stronger impact on secondary crisis communications (Wang & Wanjek, 2018). Therefore, privacy concerns could also be related to secondary crisis communications. Due to the assumption that privacy concerns can be seen as a negative tendency towards perceptions, this study suggests that it has a positive tendency towards secondary crisis communications. Accordingly, the following hypotheses can be stated:

H5a: When there is a data breach crisis, a high individual privacy concern has a stronger impact on weakening the perception on organizations compared to a low individual privacy concern.

H5b: When there is a data breach crisis, a high individual privacy concern has a stronger impact on secondary crisis communication compared to a low individual privacy concern.

2.7 Conceptual model

A conceptual model is created to clarify the relationships between the different variables presented in the hypotheses mentioned earlier.

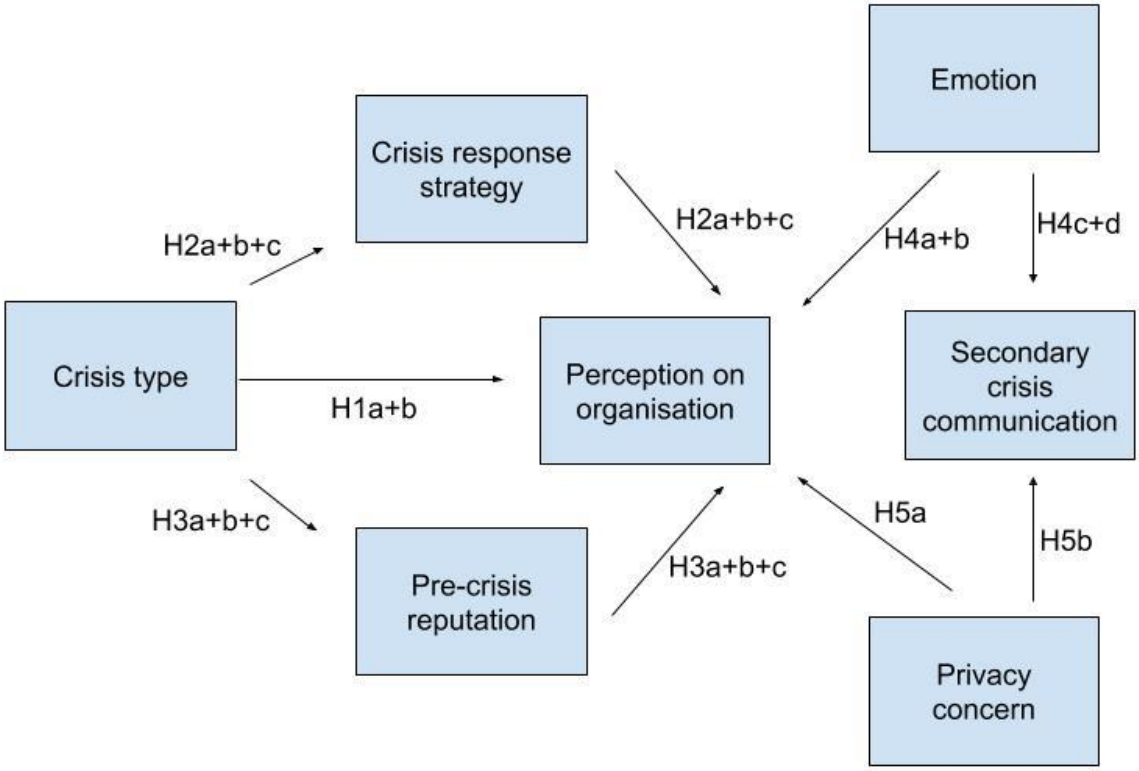


Figure 1: Research overview

3. Methodology

3.1 Research design

To answer the proposed research questions, a quantitative research method was being conducted. The reason for choosing this method is because previous research on crisis communication had mostly focused on using case study methods, which were difficult to generalize and did not offer enough theoretical understanding of crisis communication (Kiambi & Shafer, 2016). To understand the participant's perception in the context of the research questions of this study and to examine causality, it was necessary to use experimental design methods which could investigate the effects of three types of data breaches (intentional and internal, unintentional and internal, intentional and external), two crisis response strategies (denial and no response), the pre-crisis reputation of the organization (high and low), emotion towards the organization (anger and sympathy) and individual privacy concern (high and low). In that way, the outcoming data could be quantified and statistically analyzed to expose the causal relationships between the variables (Avery, Lariscy, Kim & Hocke, 2010). Using online participants to gather data for this research was especially useful when considering perceptions on and reactions to online content such as the fictitious online newspapers used in this study (Neuman, 2014).

In order to test the hypotheses, a few variables were included in the analysis. A factorial design with twelve conditions was being used, in which a **3 data breach crisis** (intentional and internal vs. unintentional and internal vs. intentional and external) **X 2 crisis response strategies** (denial vs. no response) **X 2 pre-crisis reputations** (high vs. low) between-subjects design is selected. Emotion towards an organization and individual privacy concerns could be seen as additional effects in this context.

Table 3.1: Research conditions

		Intentional & Internal data breach crisis	**Unintentional & Internal data breach crisis**	**Intentional & External data breach crisis**
Denial response strategy	**High pre-crisis reputation**	*Condition 1*	*Condition 2*	*Condition 3*
	Low pre-crisis reputation	*Condition 4*	*Condition 5*	*Condition 6*
No response strategy	**High pre-crisis reputation**	*Condition 7*	*Condition 8*	*Condition 9*
	Low pre-crisis reputation	*Condition 10*	*Condition 11*	*Condition 12*

3.2 Sampling and data collection

3.2.1 Pre-test

Before conducting the experiment and collecting data, a pre-test has been done to make sure that the questions in the experiment were clear to the different participants and that all the twelve conditions could be easily distinguished due to the manipulations in the stimulus material. In this way, after the participants processed the information of the different experimental conditions, some questions were being asked to make sure that misunderstandings were being prevented, and that there was no ineffective data present in the experiment. The pre-test was implemented on the 24th March 2020 among 7 participants filling in the survey on a mobile phone, laptop, or computer, using a shared link via email. The data of these surveys were not used in the final dataset. These 7 participants also received a PDF-file of all the twelve experimental conditions and were being asked whether they could answer the manipulation check questions and whether the distinction was clear, given the information provided in the experimental conditions. After conducting the pre-test among the 7 participants and receiving feedback, some small changes in the surveys were made. Some sentences were a bit

unclear to the participants, therefore, its structure has been changed to a more general level. Furthermore, the font for the newspaper articles was too small to read when conducting the survey. Therefore, to fix this misapprehension, the image of the news article was corrected by enlarging the pixels to make it easier for the participants to read on their laptop, computer, and mobile phone.

3.2.2 Sample

For the final experiment, a non-probability convenience sampling method was chosen to be conducted because it is a natural, inexpensive, and quick way to gather data. An online crowdsourcing platform has been used to conduct the convenience sampling. Crowdsourcing can be seen as an online, distributed problem-solving model that approaches crowds and asks for contributions to help organizations, or in this case, academics, by overcoming challenges (Prpic, Shukla, Kietzmann & McCarthy, 2015). Crowdsourcing platforms are online websites that can be used to ask online workers to conduct some small tasks in exchange for small financial stimulations (Kohler & Chesbrough, 2019). These platforms could be used to make sure that the data set contains diversity in fields of different demographics like nationality, education, and age (Ross, Irani, Silberman, Zaldivar & Tomlinson, 2010). The online crowdsourcing platform that has been used and recruited the participants for this experiment was the largest and well-known platform, called Amazon Mechanical Turk (MTurk). Amazon Mechanical Turk is considered as a valid and reputable source for data collection because it has some features that make sure the occurring data is useful, like the power of the researcher to accept (pay) or reject (not pay) the submitted work, the identification of others and the contribution to each other's reputation by requesters and workers. Also, workers have diverse nationalities, which allows cross-cultural comparative research (Buhrmester, Kwang & Gosling, 2011; Lowry, D'Arcy, Hammer & Moody, 2016; Shank, 2015). Therefore, this method has been used to increase the diversity and representativeness of the sample. In this way, the confidence increased that the groups are not systematically different, now that each case has the same chance of being selected (Neuman, 2014). Besides that, the use of the online software of Amazon Mechanical Turk made sure that there was no tilting situation towards the

researcher's background and that there was no influence on the results by a biased and non-representative sample (Neuman, 2014). Although convenience sampling is regarded as a method that delivers less generalizable results than other sampling methods, the use of Amazon Mechanical Turk improves the external validity by recruiting a greater variety of participants (Shank, 2015).

Each condition of the experiment would need to fulfill the expectation of recruiting 30 participants, which meant that a total of 360 participants were needed for all twelve experimental conditions (Box, 1980). Since some drop-outs occurred, and some workers failed in answering the manipulation check questions, the experiment attempted to gather data from 500 participants. Eventually, the experiment collected N = 709 between March 30th 2020, and April 8th 2020, from which N = 563 were being used after data cleaning. To increase the internal validity of the study, data cleaning was conducted by firstly deleting all participants that finished the experiment within two minutes (N = 70), for the reason that the answers of these participants are being seen as unreliable. Secondly, the participants were deleted that did not answer one or more questions in the experiment (N = 76). The experiment was set up by using Qualtrics, an online surveying platform. In combination with Amazon Mechanical Turk, these platforms conducted an online experiment that reached a wide range of participants with the absence of interviewer bias inexpensively and conveniently (van Selm & Jankowski, 2006).

3.3 Experimental scenarios

To create the twelve conditions for the experimental design, fictitious newspaper articles were being developed and used. These news articles focused on one of the three different data breach crises, conducted by one of the two high or low reputational organizations that used one of the two response strategies. The New York Times was chosen as the newspaper brand that fictionally posted the article on its website. The reason for choosing The New York Times was because this brand is one of the most widely read newspapers in the United States, has won far more Pulitzer Prizes than any other media company in U.S. history and scores high on perceptions of the publication's trustworthiness due to its accuracy in reporting (Watson, 2019).

The substantive choices of the newspaper articles about the different data breach crises were based on the classification table in the article by Confente et al (2019). For the intentional and internal data breach, the table sketched the context about an insider, for example, an employee, contractor, or customer, with legitimate access that intentionally breaches information (Confente et al., 2019; Coombs & Holladay, 1996, 2001; Sen & Borle, 2015). For this experiment, the example of an employee that steals data intentionally was being used. For the unintentional and internal data breach, the table in the article of Confente et al talked about the unintended disclosure of information by the organization, not included hacking, intentional breach, or physical loss (2019). The examples given were sensitive information posted publicly, mishandled, or sent to the wrong party via publishing online, sending in an email, sending in a mailing or sending via fax (Confente et al., 2019; Coombs & Holladay, 1996, 2001; Sen & Borle, 2015). For this experiment, an employee that accidentally discloses data by posting sensitive information in public was being utilized. Finally, for intentional and external data breach the table of Confente et al talked about fraud involving debit and credit cards that was not practiced by hacking, hacking by an outside party or infection by malware (Confente et al., 2019; Coombs & Holladay, 1996, 2001; Sen & Borle, 2015). For the experiment, an article about hacking by an outside party was being used.

Also, the news articles were focused on either a high reputation or on a low reputation organization. The American multinational technology company Google was chosen as a high reputation organization. Google is the most frequently-used search engine in the world, which also operates in cloud computing, online advertising technologies, software, and hardware. Using Google for the high pre-crisis reputation conditions was being made on behalf of the fact that this organization has the best reputation for corporate responsibility globally, according to Reputation Institute's 2018 Global CR RepTrak 100 Rankings study (Czarnecki, 2018). The reason for using an existing organization was because the concept of reputation evolves over time. This constantly changing phenomenon is difficult to forge in the experimental design (Fombrun, Gardberg & Sever, 2000). For the Google conditions, some manipulation check questions were included to check if the participant has the image of a high

reputation towards Google. For the low reputation organization, a fictitious brand called SearchLand was used that was, therefore, unknown to the participants of the experiment.

To manipulate the crisis response strategy, the newspaper articles contained a part stating that the organization denies the crisis or, in the other case, the crisis response was missing. For the denial response strategy, the article ended with: “... is unclear due to the fact that Google/SearchLand denies the existence of this data breach accident”. For the no response strategy, the article ended with: “... is unclear due to the fact that Google/SearchLand refuses to respond to the data breach accident”.

Despite the three manipulations of data breach crises, high or low reputation organizations, and crisis response strategies, the content of the newspaper articles was being kept as similar as possible. In every condition, the article claimed that personal information of 18.000 users was being exposed publicly on the Internet for two whole days, including personal details like names, gender, age, dates of birth, and e-mail addresses. By keeping this information the same on every condition, it was assured that only the manipulations influenced the experiment results.

3.4 Operationalization

The experiment started with an introductory text to better understand the content of the experiment and its purposes. A guarantee of anonymity was shown so the participant could be sure that his or her personal information was kept strictly confidential. Also, the contact information about the researcher and the research institution was presented in the introductory text. After agreeing to the terms, the participant was assigned to one of the twelve conditions and started with completing the survey by answering the main questions, which will be discussed below. In this experiment, three independent variables were manipulated, namely the three different types of data breach crisis, two crisis response strategies, and two levels of pre-crisis reputation organizations. The variables that were measured in the experiment included privacy concern, pre-crisis reputation, perception on organizations, anger, sympathy, corporate crisis responsibility, secondary crisis communication, and some demographic variables. The scales that were being used for measuring these features were validated

in previous research. The experiment ended with a debriefing consisting of a message thanking the participant for contributing to the experiment and a note about the fictionality of the newspaper articles.

3.4.1 Manipulation checks

After the main questions in the experiment, three manipulation checks of data breach crisis, crisis response strategy, and pre-crisis reputation were being conducted to make sure that all the manipulations on the dependent variables were successful. To check the manipulations and to facilitate the following analyses, dummy variables were created for the twelve conditions, based on the three types of data breach crisis (0 = intentional and internal, 1 = unintentional and internal, 2 = intentional and external), two crisis response strategies (0 = denial response, 1 = no response) and two pre-crisis reputation organizations (0 = high pre-crisis reputation, 1 = low pre-crisis reputation).

For the three types of data breach crisis, participants that were in the intentional and internal, unintentional and internal or intentional and external conditions had to answer that this was the data breach crisis they observed in the newspaper article. This check was conducted by asking the participants the following question: 'Which crisis type did you read in the newspaper article?'. The participants could answer 'employee steals data intentionally', 'employee accidentally discloses data' or 'hacking incident by outside party'. The complete dataset consisted of 563 participants, from which 186 participants were distributed to the intentional and internal conditions, and 156 passed the manipulation check (83.9%). For the unintentional and internal conditions,187 participants were distributed, and 168 passed the manipulation check (89.8%). Subsequently, 190 participants were distributed to the intentional and external conditions, from which 153 passed the manipulation check (80.5%). To finalize, when analyzing the Pearson Chi-square value in the crosstab, the manipulation of data breach crisis was measured. This showed that there was a significant effect, χ^2 (4, N = 563) = 676.08, p <.001. This significant effect meant that the data breach variable succeeded in the manipulation with 95% certainty.

The following manipulation check was focused on the manipulation effect of crisis response strategies. At the end of the newspaper article, participants were provided

with information about how the organization responded to the crisis. By asking the question ‘What did the organization respond to the crisis in the newspaper article?’, participants had to answer what they observed in the newspaper article, choosing between ‘denies the existence of the accident’ or ‘refuses to respond to the accident’. From a total of 563 participants, 275 participants were distributed to the denial response condition, from which 191 participants passed the manipulation (69.5%), and 288 participants were distributed to the no response condition, from which 220 passed the manipulation (76.4%). The Pearson Chi-square test value demonstrated a significant effect, χ^2 (1, N = 563) = 119.02, p <.001. This meant that the crisis response strategy variable also succeeded in the manipulation with 95% certainty.

The following manipulation check was created to test whether the manipulation for pre-crisis reputation was successful. The newspaper articles were reporting on either a high reputation organization (Google) or a low reputation organization (SearchLand). Participants were asked the question: ‘What was the name of the company in the newspaper article?’ to check if the manipulation was successful. They could choose between ‘Google’ or ‘SearchLand’. Of the 563 participants, 283 participants were distributed to the condition of the high reputation organization Google, from which 272 participants passed the manipulation check (96.1%). Besides, 280 participants were distributed to the condition of the low reputation organization SearchLand, and 256 participants passed the manipulation check (91.4%). The Pearson Chi-square test value demonstrated a significant effect, χ^2 (1, N = 563) = 432.59, p <.001. This meant that the pre-crisis reputation variable also succeeded in the manipulation with 95% certainty.

3.4.2 Measurements

Privacy concern. Before the participant was exposed to one of the twelve conditions, which showed one of the twelve newspaper articles, he or she was tested on individual privacy concerns in general. To measure this individual privacy concern, a 5-point scale ranging from 1 (not at all) to 5 (extremely) about the attitude dimension of the “Adapted Scale for Online Privacy Concern and Protection” (APCP) by Taddicken was being used (2010). This scale comprised 17 questions about attitudes towards online privacy and indicated the general concept of individual privacy concerns. A

selection of five questions has been made: ‘In general, how concerned are you about your privacy while using the Internet?’, ‘Are you concerned that you are asked for too much personal information when you register or make online purchases?’, ‘Are you concerned about online identity theft?’, ‘Are you concerned about people you do not know obtaining personal information about you from your online activities?’ and ‘Are you concerned that personal content that you store securely on the Internet (e.g., photos) can be viewed by others?’ (Taddicken, 2010).

A reliability test was conducted to validate the scale. For this reliability test, a Cronbach’s alpha above 0.7 was needed (Pallant, 2014). The Reliability statistics table indicated a Cronbach’s alpha of 0.869 for the newly created scale “Privacy concern” (*M* = 3.62, *SD* = 0.84), which was therefore reliable (Pallant, 2014).

After the reliability test, a Factor analysis in the form of a principal component analysis with varimax rotation has been conducted to measure that one component had an Eigenvalue of 3.291 and explained 65.8% of the variance. The other four components were all insignificant because of their Eigenvalue < 1. Therefore, a new measure was created based on this analysis, namely *Privacy Concern,* which ranged from 1 = not at all to 5 = extremely.

Table 3.4.2: Privacy concern Factor Loading

Are you concerned about people you do not know obtaining personal information about you from your online activities?	.850
Are you concerned about online identity theft?	.825
In general, how concerned are you about your privacy while using the Internet?	.812
Are you concerned that personal content that you store securely on the Internet (e.g. photos) can be viewed by others?	.804
Are you concerned that you are asked for too much personal information when you register or make online purchases?	.762

Pre-crisis reputation. Dependent on the organization in the newspaper article, the question was asked, 'Do you know Google?' (condition 1, 2, 3, 7, 8, and 9) or 'Do you know the brand SearchLand?' (condition 4, 5, 6, 10, 11, and 12) to check the manipulation. For the Google conditions, to check if Google was perceived as an organization with a high pre-crisis reputation, four questions were asked to measure if the participants like, trust and admire the organization (Ponzi, Fombrun & Gardberg, 2011). The four questions were as follows: 'Google is a company I have a good feeling about', 'Google is a company that I trust', 'Google is a company that I admire and respect' and 'Google has a good overall reputation'. These four questions were only asked to participants randomized to the high pre-crisis reputational conditions 1, 2, 3, 7, 8, and 9. To validate this scale, a reliability test was being conducted. The Cronbach's alpha for this analysis was 0.918, which meant that the scale could be seen as reliable (Pallant, 2014). This implied that for every high pre-crisis condition, the four items could be combined into a mean scale "Pre-crisis reputation" (M = 5.43, SD = 1.21).

Also, the principal components analysis with varimax rotation was conducted on these four measures in every high pre-crisis reputation condition. This analysis showed that one component had an Eigenvalue > 1, namely 3.216. This explained 80.4% of the variance. The other three components were negligible (Eigenvalue <1). A new measure was created for the high pre-crisis reputation conditions based on these analyses: *Pre-crisis Reputation,* which ranged from 1 = strongly disagree to 7 = strongly agree.

Table 3.2.3: Pre-crisis Reputation Factor Loading

Google is a company I have a good feeling about.	.924
Google is a company that I trust.	.917
Google is a company that I admire and respect.	.898
Google has a good overall reputation.	.846

Perception on organization. To continue, the participants were shown one of the twelve fictitious newspaper articles about a data breach crisis (intentional and internal vs. unintentional and internal vs. intentional and external) happening at one of the organizations (Google vs. Searchland) that used one of the crisis response strategies

(denial vs. no response). After reading this, the participants were asked to leave their opinions about the organization in the newspaper article. To measure the perceptions of the participants on the organization, a 7-point semantic differential scale ranging from 1 to 7 with six items was being used based on the study of Boerman, Reijmersdal, and Neijens (2012). The participants were asked to select, after the question 'I associate the company in the newspaper article as …', to what extent the items about the organization were in their perception bad/good, unpleasant/pleasant, unfavorable/favorable, negative/positive, to dislike/like, as poor/high quality. To validate the scale, a reliability test was conducted. Analyzing the Reliability statistics table, it showed a Cronbach's alpha of 0.961, which means that the scale was highly reliable (Pallant, 2014). In order, all the items were merged into a mean scale "Perception on organization" (M = 3.33, SD = 1.47).

Furthermore, the Factor analysis (principal component with varimax rotation) explained that one component had an eigenvalue of 5.027 and explained 83.8% of the variance. The other five components were negligible because their Eigenvalue was below 1. In this way, a newly created overarching measure has emerged: *Perception on Organization,* which ranged from 1 = very (*negative factor)* to 7 = very (*positive factor*).

Table 3.2.4: Perception on organization Factor Loading

Unfavorable/Favorable	.933
Negative/Positive	.931
Unpleasant/Pleasant	.927
Dislikeable/Likeable	.922
Bad/Good	.903
Poor Quality/High Quality	.875

Anger and Sympathy. During the following part of the experiment, the data about emotions of participants towards the organization was being measured by using a 7-point Likert scale, ranging from 1 (not at all) to 7 (extremely) with four items based on

anger and four items based on sympathy (McDonald, Glendon & Sparks, 2011). This scale was created and tested, especially for crisis emotion. Participants had to complete the following statement: 'When I think about the company, I feel…'. The anger scale contained the items angry, disgusted, annoyed, and outraged and the sympathy scale contained the items sympathetic, sorry, compassion, and empathy (McDonald et al., 2011). The four items belonging to the "Anger" scale were included in the reliability test, which led to a Cronbach's alpha of 0.930. This meant that the scale was highly reliable (Pallant, 2014). The four items belonging to the "Sympathy" scale were also included in the reliability test, which led to a Cronbach's alpha of 0.903. This meant that the scale was also highly reliable (Pallant, 2014). The items were combined into two new mean scales which were named "Anger" (*M* = 4.13, *SD* = 1.67) and "Sympathy" (*M* = 3.11, *SD* = 1.56).

A Factor analysis has been done on these two scales with every four measures. For the anger scale, one component had an Eigenvalue of 3.307 and explained 82.7% of the variance. For the sympathy scale, one component had an Eigenvalue of 3.103 and explained 77.6% of the variance. For both scales, the other three components had an Eigenvalue below 1. In this way, two newly created overarching measures have emerged: *Anger* and *Sympathy,* which ranged from 1 = not at all to 7 = extremely.

Table 3.2.5: Anger Factor Loading

Angry	.924
Outraged	.914
Disgusted	.903
Annoyed	.895

Table 3.2.6: Sympathy Factor Loading

Empathy	.926
Compassion	.905
Sympathetic	.845
Sorry	.845

Corporate Crisis Responsibility. Also, the perceived corporate crisis responsibility of the organization in the experiment has been measured by using the "Blame scale" (Griffin, Babin & Darden, 1992). This scale consisted of three different items, namely 'Circumstance, not the company, are responsible for the crisis', 'The blame for the crisis lies with the company' and 'The blame for the crisis lies in the circumstances, not the company'. The second question was reversed to resolve the problem of an incompatible scale. These statements could be answered by using a 7-point scale from 1 (strongly disagree) to 7 (strongly agree). A reliability test has been conducted to validate the scale, which resulted in a Cronbach's alpha of 0.710. This means that the scale was reliable (Pallant, 2014). Therefore, the three items emerged into a mean scale, which was called "Corporate crisis responsibility" (*M* = 3.24, *SD* = 1.33).

The Factor analysis on these three measures explained that one component has an Eigenvalue of 1.919, and this explained 64.0% of the variance. The other two components were negligible because their Eigenvalue was below 1. Also, a new measure was being created based on this analysis: *Corporate Crisis Responsibility* ranging from 1 = strongly disagree to 7 = strongly agree.

Table 3.2.7: Corporate Crisis Responsibility Factor Loading

The blame for the crisis lies in the circumstances, not the company.	.902
Circumstances, not the company, are responsible for the crisis.	.875
The blame for the crisis lies with the company.	.584

Secondary Crisis Communication. Measurements for secondary crisis communication were based on a 7-point Likert scale from 1 (strongly disagree) to 7 (strongly agree), including three items (Schultz et al., 2011). These items were somewhat adapted to match the experimental conditions and were described as: 'I would like to share the news with other people', 'I would like to tell my friends about the incident' and 'I would like to leave a reaction to this news'. Thus, this scale measured no opinions of the participants, but reactions and intentions to take action after the

occurrence of a crisis. The Reliability statistics table presented a Cronbach's alpha of 0.877, which meant that the scale was reliable (Pallant, 2014). Therefore, all three items were merged into a mean scale called "Secondary crisis communication" (*M* = 4.58, *SD* = 1.53).

The Factor analysis, focused on a principal component analysis with varimax rotation, found that one component had an Eigenvalue of 2.420 and explained 80.7% of the variance. The other two components were negligible because their Eigenvalue was below 1. The next step was the creation of a new measure called: *Secondary Crisis Communication* ranging from 1 = strongly disagree to 7 = strongly agree.

Table 3.2.8: Secondary Crisis Communication Factor Loading

I would like to tell my friends about the incident.	.928
I would like to share the news with other people.	.925
I would like to leave a reaction to this news.	.838

3.5 Reliability and validity

To increase the reliability and validity of this study, some measures were embraced. To start with, reliability was being considered to make the study more dependable or consistent (Neuman, 2014). Internal reliability was strengthened by conducting data cleaning to delete all the defective samples in the dataset. Also, to strengthen the internal consistency and the reliability of the scales, which combined multiple items, two different analyses were conducted. The factor analysis made sure that the observed variables, which were strongly correlated with each other, were grouped. On the other hand, the reliability analysis, including a high Cronbach's alpha, confirmed that the different groups of observed variables did go well together. To increase the external reliability of the experiment, this study could build on the fact that it was conducted in an online environment, which makes it more convenient for other researchers to imitate the experiment.

It was also essential to take the validity of this research into account, which means that it had to be truthful to the extent that an idea fitted with the actual reality

(Neuman, 2014). To start with, some measures in the experiment strengthened the internal validity of the experiment. The scales that were being used in this study were developed based on relevant existing knowledge and literature. Because the different measurements of the study consisted of multiple items, triangulation was reached since this study observed the participant from multiple perspectives instead of only a single perspective (Neuman, 2014). Moreover, manipulation check questions (hypotheses 1, 2, and 3) and control variables (hypotheses 4 and 5) were included to make sure that only the independent variables affected the dependent variables by isolating external factors. A pre-test of the experiment stimuli has been done to verify that the manipulations were representable for the experimental outcomes. Besides, by using the randomization feature of the online tool Qualtrics, the representativeness of the sample increased due to the random assignment of the twelve conditions excluding the possibility of participants causing bias. To strengthen the external validity of the experiment, the online crowdsourcing tool of Amazon Mechanical Turk made sure that the participants were diversified on their demographic features. In this way, a sample was created that came close to the general population (Neuman, 2014).

3.6 Description and demographics

The data collected included 709 participants in total (N = 709), 146 participants were deleted due to completing the survey within two minutes or failing to answer some of the questions. In the end, the used dataset consisted of N = 563 participants who have taken the time to complete the survey successfully. After analyzing the demographics, it showed that 337 participants were male (59.9%), and 226 participants were female (40.1%), which means males were represented more often in the partition of the experiment. Besides, when looking at the dataset, it showed that the mean age of the participants was M = 36.02, ranging from 17 to 74 years, with SD = 12.134. In the end, when analyzing the level of education, it showed that most participants (N = 220) obtained a Master's degree (39.1%), followed by 163 participants who obtained a Bachelor's degree (29.0%). The dataset showed for education level a mean of M = 4.28 and a standard deviation of SD = 1.184.

From the 283 participants in the high pre-crisis reputation, all of the 283 participants knew the brand Google (100.0%). Also the result on the 7-point scale questions, regarding the variable of *Pre-crisis Reputation,* indicated that the participants gave the high pre-crisis organization Google an above-average reputational score (*M* = 5.43, *SD* = 1.21) since the average score of this scale is 3.5.

Table 3.5: Correlation Matrix

Variables	Privacy concern	Pre-crisis rep.	Perception org.	Anger	Symp. athy	Corporate crisis resp.	Sec. crisis com.	Age	Gender	Education
Privacy concern	1									
Pre-crisis rep.	.056	1								
Perception on org.	-.075	.353**	1							
Anger	.234**	-.073	-.438**	1						
Sympathy	.010	.372**	.375**	.031	1					
Corporate crisis resp.	-.101*	.272**	.483**	-.340**	.374**	1				
Sec. crisis com.	.231**	.276**	.145**	.314**	.143**	-.124**	1			
Age	-.077	-.120*	-.077	-.027	-.208**	-.085*	-.147*	1		
Gender	-.073	.005	-.080	.011	-.116**	.023	-.023	.131**	1	
Education	.118**	.156**	.065	-.018	.138**	.058	.039	-.005	-.019	1

* Correlation is significant at the 0.05 level (2-tailed).
** Correlation is significant at the 0.01 level (2-tailed).

Looking at the correlation matrix, it showed that between the main variables, there were several correlations significant. These main variables were also correlated with the demographic variables age, gender, and education level. Since most significant correlations were situated at the p<.01 level, these were the only reported correlations. First of all, there was a moderate positive correlation between '*Perception on Organization'* and *'Pre-crisis Reputation'* (r=0.353). Besides, '*Anger'* was weakly

positively correlated with *'Privacy Concern'* (r=0.234) and moderately negatively correlated with '*Perception on Organization'* (r=-0.438). '*Sympathy'* was found to be moderately positively correlated with *'Pre-crisis Reputation'* (r=0.372) and '*Perception on Organization'* (r=0.375). Furthermore, *'Corporate Crisis Responsibility'* was weakly positively correlated with *'Pre-crisis Reputation'* (r=0.272), moderately positively correlated with *'Perception on Organization'* (r=0.483) and *'Sympathy*' (r=0.374), and moderately negatively correlated with *'Anger'* (r=-0.340). Also, *'Secondary Crisis Communication'* was weakly positively correlated with *'Privacy Concern'* (r=0.231), *'Pre-crisis Reputation'* (r=0.276), *'Perception on Organization'* (r=0.145) and *'Sympathy'* (r=0.143), moderately positively correlated with *'Anger'* (r=0.314) and weakly negatively correlated with *'Corporate Crisis Responsibility'* (r=-0.124). Next, *'Age'* was weakly negatively correlated with *'Sympathy'* (r=-0.208). Besides, *'Gender'* was weakly negatively correlated with *'Sympathy'* (r=-0.116) and weakly positively correlated with *'Age'* (r=0.131). To finalize, *'Education'* was weakly positively correlated with *'Pre-crisis Reputation'* (r=0.156) and *'Sympathy'* (r=0.138).

3.7 Data analysis

When all the adequate data was collected, the results were analyzed through SPSS (version 24), which could be described as a statistical software package for data analysis. For hypotheses 1 the One-way ANOVA test was run, and for hypotheses 2 and 3 the Two-way ANOVA test was conducted. An advantage of this factorial design was that, besides the main effects of the variables, the interaction effects between different combinations of variables could be exposed (Neuman, 2014). Afterwards, for hypotheses 4 and 5, regression analyses were conducted. At the end, additional regression analyses were performed to measure the control variables for hypotheses 4 and 5.

4. Results

4.1 Hypotheses 1: The impact of data breach crisis on the perception on organizations

H1a hypothesized that intentional and internal data breaches had a stronger impact on weakening the perception on organizations than unintentional and internal data breaches as well as intentional and external data breaches. Also, H1b hypothesized that unintentional and internal data breaches had a stronger impact on weakening the perception on organizations than intentional and external data breaches. Levene's test showed that an equal variance was assumed between data breach crisis and perception on organization, F (2, 560) = 1.89, p = .152. Based on these assumptions, an One-way ANOVA was conducted to compare the effect of type of data breach crisis on the perception on the organization situated in a data breach crisis. An analysis of variance showed that the effect of data breach crisis on the perception on organizations was close to significant at the p<.05 level: F(2, 560) = 2.99, p = .051, η2 = 0.01.

Table 4.1: Results of One-way ANOVA Data Breach Crisis (N = 563)

	Sum of Squares	*df*	Mean Square	*F*	*p*	*η2*
Between Groups	12.776	2	6.388	2.987	.051	.011
Within Groups	1197.548	560	2.138			
Total	1210.324	562				

**p<.1, **p<.05, ***p<01*

A Tukey post hoc test revealed that an intentional and internal data breach crisis caused a perception on the organization that was statistically significantly weaker (M = 3.15, SD = 1.50) compared to the perception on the organization after an intentional and external data breach (M = 3.52, SD = 1.52) with a p-value of 0.040. There was no statistically significant difference between perceptions on the organization after an unintentional and internal data breach crisis (M = 3.31, SD = 1.37) and an intentional and internal data breach crisis (p = 0.565) or intentional and external data breach crisis

(p = 0.335). Because of this, H1a, saying that there is a stronger impact on weakening the perception of the participants on organizations within an intentional and internal data breach crisis compared to an unintentional and internal data breach as well as an intentional and external data breach, was partly rejected. This was because it demonstrated a close to significant result in the ANOVA test, but a partly significant and insignificant result in the post hoc tests. Besides, H1b, saying that there is a stronger impact on weakening the perception of participants on organizations within an unintentional and internal data breach crisis than an intentional and external data breach, was rejected because it demonstrated insignificant results. However, the results showed that there was a statistically significant difference between an intentional and internal data breach crisis and an intentional and external data breach crisis. Therefore, it could be stated that an intentional and internal data breach crisis caused a stronger impact on weakening the perception of the participants on organizations than an intentional and external data breach crisis.

4.2 Hypotheses 2: The impact of crisis response strategy on the perception on organizations

H2a hypothesized that within an intentional and internal data breach crisis, a no response strategy had a stronger impact on weakening the perception on organizations compared to a denial response strategy. According to hypothesis H2b and H2c, the same situation occurred within an unintentional and internal data breach crisis as well as an intentional and external data breach crisis. A denial response strategy (M = 3.31, SD = 1.50) appeared to result in a weaker perception on organizations than a no response strategy (M = 3.35, SD = 1.43). Levene's test showed that an equal variance was assumed between the conditions, F (5, 557) = 1.96, p = .083. Based on these assumptions, a Two-way ANOVA was conducted to compare if data breach crisis (Fixed Factor 1) in combination with crisis response strategy (Fixed Factor 2) affected the perception on organizations (DV). An analysis of variance showed that type of data breach crisis had an insignificant effect on the perception on organizations, F (2, 557) = 2.998, p = .051, η2 = 0.01 and there was no significant effect with respect to crisis response strategy, F (1, 557) = 0.15, p = .697, η = 0.00. Furthermore, the interaction

effect between data breach crisis and crisis response strategy on the perception on the organization was not significant at the p<.05 level: F(2, 557) = 0.52, p = .595, η2 = 0.00.

Table 4.2: Results of Two-way ANOVA Data Breach Crisis and Crisis Response Strategy (N = 563)

	Sum of Squares	*df*	Mean Square	*F*	*p*	*η2*
Data Breach Crisis	12.864	2	6.432	2.998	.051	.011
Crisis Response Strategy	.325	1	.325	.151	.697	.000
Data Breach Crisis * Crisis Response Strategy	2.233	2	1.117	.520	.595	.002
Error	1195.003	557	2.145			
Total	7450.333	563				

**p<.1, **p<.05, ***p<.01*

This meant that the difference between the perception on organizations after a denial response strategy within an intentional and internal data breach crisis (*M* = 3.12, *SD* = 1.63), unintentional and internal data breach crisis (*M* = 3.21, *SD* = 1.40) and intentional and external data breach crisis (*M* = 3.58, *SD* = 1.46) or after a no response strategy within an intentional and internal data breach crisis (*M* = 3.18, *SD* = 1.37), unintentional and internal data breach crisis (*M* = 3.40, *SD* = 1.34) and intentional and external data breach crisis (*M* = 3.46, *SD* = 1.58) were statistically insignificant. Because of this, H2a, H2b, and H2c, saying that within all of the three types of data breach crisis, there was a stronger impact on weakening the perception on organizations if a no response strategy was conducted compared with a denial response strategy, were rejected as the results from this analysis demonstrated that a no response strategy did not provide significant results compared to a denial response strategy.

4.3 Hypotheses 3: The impact of pre-crisis reputation on the perception on organizations

H3a hypothesized that within an intentional and internal data breach crisis, a low pre-crisis reputation of an organization had a stronger impact on weakening the perception on the organization compared to a high pre-crisis reputation of an organization. According to H3b and H3c, the same situation occurred within an unintentional and internal data breach crisis as well as an intentional and external data breach crisis. A high pre-crisis reputation (M = 3.58, SD = 1.40) appeared to result in a better perception on organizations than a low pre-crisis reputation (M = 3.07, SD = 1.49). Levene's test showed that an equal variance was assumed between data breach crisis and perception on organization, F (5, 557) = 1.22, p = .296. Based on these assumptions, a Two-way ANOVA was conducted to compare if data breach crisis (Fixed Factor 1) in combination with pre-crisis reputation (Fixed Factor 2) affected the perception on organizations (DV). An analysis of variance showed that type of data breach crisis had a significant effect on the perception on organizations, F (2, 557) = 3.12, p = .045, η2 = 0.01 and there was a significant, but weak effect with respect to pre-crisis reputation, F (1, 557) = 17.97, p <.001, η2 = 0.03. Furthermore, the interaction effect between data breach crisis and pre-crisis reputation on the perception on the organization was not significant at the p<.05 level: F(2, 557) = 0.16, p = .849, η2 = 0.00.

Table 4.3: Results of Two-way ANOVA Data Breach Crisis and Pre-crisis Reputation (N = 563)

	Sum of Squares	*df*	Mean Square	*F*	*p*	*η2*
Data Breach Crisis	12.999	2	6.499	3.122	.045*	.011
Pre-crisis Reputation	37.410	1	37.410	17.971	.000**	.031
Data Breach Crisis * Pre-crisis Reputation	.683	2	.341	.164	.849	.001
Error	1159.493	557	2.082			
Total	7450.333	563				

**p<.1, **p<.05, ***p<.01*

These results meant that the difference between the perception on organizations with a high pre-crisis reputation (*M* = 3.58, *SD* = 1.40) or with a low pre-crisis reputation (*M* = 3.07, *SD* = 1.49) was statistically significant, regardless of the data breach crisis in which an organization occurred. Because of this, H3a, H3b, and H3c, saying that within all of the three types of data breach crisis, there was a stronger impact on weakening the perception on organizations if it had a low pre-crisis reputation compared with a high pre-crisis reputation, were accepted. This could be stated because the results from this analysis demonstrated that low pre-crisis reputation did provide significant results compared to high pre-crisis reputation.

4.4 Regression analyses for testing H4 and H5

The computed variables were standardized to adjust them for variances in the scales by using SPSS. These *z-score* variables were used to support the following regression analysis. The assumptions for these regression analyses were satisfied. The normal probability plots for each regression analysis were examined. The visualizations of these plots were inspected, and they all revealed that the assumption of normality of errors was met. Also, tests to see if the data met the assumption of collinearity indicated that multicollinearity was not a concern.

4.4.1 Hypotheses 4: The impact of emotion on the perception on organizations and secondary crisis communication

H4a hypothesized that in a data breach crisis, more anger towards an organization had a stronger impact on weakening the perception of organizations compared to less anger. In contrast, H4b hypothesized that in a data breach crisis, more sympathy towards an organization had a stronger impact on strengthening the perception on organizations compared to less sympathy. A multiple regression analysis was conducted to investigate if anger or sympathy could significantly predict perceptions on organizations. The results of the regression analysis revealed an R-square value of .341, which showed that the two different variables explained 34.1% of the variance and that these two variables predicted perceptions on organizations significantly, $F(2, 560) = 146.17$, $p < .001$. The variable of anger was statistically significant: $b^* = -.45$, $t = -13.15$, $p < .001$, 95% *CI* [-.52, -.38]. This result meant that with

each additional unit of anger, the perception on organizations decreased by 0.450 units. Also, the variable of sympathy was statistically significant: $b^* = .388$, $t = 11.34$, $p < .001$, 95% *CI* [.32, .46]. This result meant that with each additional unit of sympathy, the perception on organizations increased with 0.388 units.

H4c hypothesized that in a data breach crisis, more anger towards an organization had a stronger impact on secondary crisis communication compared to less anger. Also, H4d hypothesized that in a data breach crisis, more sympathy towards an organization had a stronger impact on secondary crisis communication compared to less sympathy. Another multiple regression analysis was conducted to investigate if anger or sympathy could significantly predict secondary crisis communication. The results of the regression analysis revealed an R-square value of .116, which showed that the two different variables explained 11,6% of the variance and that these two variables predicted secondary crisis communication significantly, $F(2, 560) = 36.83$, $p <.001$. The variable of anger was statistically significant: $b^* = .310$, $t = 7.80$, $p <.001$, 95% *CI* [.23, .39]. This result meant that with each additional unit of anger, secondary crisis communication increased by 0.310 units. Also, the variable of sympathy was statistically significant: $b^* = .133$, $t = 3.35$, $p = .001$, 95% *CI* [.06, .21]. This result meant that with each additional unit of sympathy, secondary crisis communication increased with 0.133 units.

4.4.2 Hypothesis 5: The impact of individual privacy concern on the perception on organizations and secondary crisis communication

H5a hypothesized that in a data breach crisis, a high individual privacy concern had a stronger impact on weakening the perception on organizations than a low individual privacy concern. A linear regression analysis was conducted to investigate if individual privacy concerns could significantly predict perceptions on organizations. The results of the regression analysis revealed a R-square value of .006 which showed that the variable explained 0.6% of the variance and that this variable predicted perceptions on organizations insignificantly, $F(1, 561) = 3.14$, $p = .077$. To specify, privacy concern had an insignificant association with perception on organizations, $b^* = -.08$, $t = -1.77$, p

= .077, 95% *CI* [-.16, .01]. Therefore, it can be stated that there is no statistically significant impact of individual privacy concerns on the perception on organizations.

Besides, H5b hypothesized that a high individual privacy concern before a data breach crisis had a stronger impact on secondary crisis communication than a low individual privacy concern. A regression analysis was conducted to investigate if individual privacy concerns could significantly predict secondary crisis communication. The results of the regression analysis revealed a R-square value of .053 which showed that the variable explained 5,3% of the variance and that this variable predicted secondary crisis communication significantly, $F(1, 561) = 31.52$, $p < .001$. To specify, privacy concern had a significant association with secondary crisis communication, $b^* = .231$, $t = 5.61$, $p < .001$, 95% *CI* [.15, .31]. This result meant that with each additional unit of privacy concern, secondary crisis communication increased with 0.231 units.

4.4.3 Additional results: control variables on perception on organizations

To facilitate a more robust analysis for H4a, H4b, and H5a, control variables including privacy concern, pre-crisis reputation of Google, anger, sympathy, corporate crisis responsibility, age, gender, and education were added in a hierarchical regression analysis. The results of the hierarchical linear regression analysis revealed a statistically significant model, $F (8, 274) = 16.34$, $p < .001$. The R-square value of 0.323 associated with this regression model suggested that some of the control variables could predict 32.3% of the differences in the perception on organizations. Pre-crisis reputation of Google, $b^* = .204$, $t = 3.69$, $p < .001$, 95% *CI* [.09, .30], anger, $b^* = -.284$, $t = -5.08$, $p < .001$, 95% *CI* [-.38, -.17], sympathy, $b^* = .268$, $t = 4.39$, $p < .001$, 95% *CI* [.14, .37] and corporate crisis responsibility, $b^* = .153$, $t = 2.69$, $p = .008$, 95% *CI* [.04, .26] had a significant correlation with perception on organizations.

Perception on organizations increased with 0.204 for every point increase in the pre-crisis reputation of Google. This resulted in a higher pre-crisis reputation of Google that will reduce the effects of a crisis on weakening the perception on organizations. Besides, perception on organizations increased with 0.153 for every point increase in corporate crisis responsibility. This resulted in the fact that the more corporate crisis responsibility can be ascribed to an organization, the stronger the effects of a crisis on

weakening the perception on organizations. To finalize, the addition of the control variables meant that with each additional unit of anger, the perception on organizations decreased by 0.284 units. Also, with each additional unit of sympathy, the perception on organizations increased with 0.268 units.

Table 4.4.3: Perception on organization Influencers

	Unstandardized B (Effect)	Standard Error	Standardized B	t-value	p (sig.)	CI (lower)	CI (upper)
Privacy Concern	.406	.052	-.047	-.893	.373	-.148	.055
Pre-Crisis Rep.	.194	.052	.204***	3.694	.000	.091	.297
Anger	-.277	.054	-.284***	-5.078	.000	-.384	-.169
Sympathy	.255	.058	.268***	4.394	.000	.141	.369
Corp. Crisis Resp.	.149	.055	.153***	2.690	.008	.040	.257
Age	.001	.004	.010	.185	.853	-.086	.103
Gender	-.096	.099	-.050	-.976	.330	-.290	.098
Education	-.050	.044	-.059	-1.146	.253	-.161	.042
R-Square	.323						
F-Test	16.338				0.000		

*p<.1, **p<.05, ***p<01.

4.4.4 Additional results: control variables on secondary crisis communication

To facilitate a more robust analysis for H4c, H4d, and H5b, control variables including privacy concern, pre-crisis reputation of Google, perception on organizations, anger, sympathy, corporate crisis responsibility, age, gender, and education were added in a hierarchical linear regression analysis. The results of the hierarchical linear

regression analysis revealed a statistically significant model, $F(9, 273) = 16.77$, $p < .001$. The R-square value of .356 associated with this regression model suggested that some of the control variables could predict 35,6% of the differences in secondary crisis communication. Privacy concern, $b^* = .105$, $t = 2.02$, $p = .044$, 95% *CI* [.00, .21], pre-crisis reputation of Google, $b^* = .246$, $t = 4.45$, $p < .001$, 95% *CI* [.14, .36], perception on organization, $b^* = .264$, $t = 4.46$, $p < .001$, 95% *CI* [.16, .40], anger, $b^* = .424$, $t = 7.42$, $p < .001$, 95% *CI* [.32, .55], corporate crisis responsibility, $b^* = -.180$, $t = -3.20$, $p = .002$, 95% *CI* [-.12, .13] and age, $b^* = -.125$, $t = -2.45$, $p = .015$, 95% *CI* [-.14, .07] had a significant correlation with secondary crisis communication. A notable point could be made about sympathy as the results showed that the addition of the control variables generated an insignificant impact of this variable on secondary crisis communication ($p = .940$). A potential explanation is that the control variables could mediate the impact of sympathy on secondary crisis communication.

Secondary crisis communication increased with 0.105 for every point increase in privacy concerns. This resulted in a higher privacy concern that raised the amount of secondary crisis communication. Secondary crisis communication increased with 0.246 for every point increase in the pre-crisis reputation of Google. This resulted in a higher perceived pre-crisis reputation of Google that raised secondary crisis communication. Also, secondary crisis communication increased with 0.246 for every point increase in perception on organizations. This signified that a better perception on organizations also raised secondary crisis communication. Besides, secondary crisis communication increased with 0.424 for every point increase in anger. This development also signified that stronger anger resulted in more secondary crisis communication. Next, secondary crisis communication decreased with 0.180 for every point increase in corporate crisis responsibility. This resulted in the fact that the more corporate crisis responsibility that could be ascribed to an organization, the lower the secondary crisis communication's intentions will be after the occurrence of a crisis. To finalize, secondary crisis communication decreased with 0.015 for every year older of the participant. This development resulted in the fact that the older the participant of the experiment, the less likely for him or her to participate in secondary crisis communication after the occurrence of a crisis.

Table 4.4.4: Secondary crisis communication Influencers

	Unstandardized B (Effect)	Standard Error	Standardized B	t-value	p (sig.)	CI (lower)	CI (upper)
Privacy Concern	.108	.054	.105**	2.021	.044	.003	.214
Pre-Crisis Rep.	.248	.056	.246***	4.454	.000	.138	.358
Perc. on Org.	.280	.063	.264***	4.473	.000	.157	.403
Anger	.438	.059	.424***	7.422	.000	.322	.554
Sympathy	.005	.062	.005	.076	.940	-.118	.127
Corp. Crisis Resp.	-.185	.058	-.180***	-3.198	.002	-.300	-.071
Age	-.010	.004	-.125**	-2.446	.015	-.220	-.024
Gender	.107	.102	.053	1.044	.297	-.095	.308
Education	-.031	.045	-.035	-.687	.493	-.142	.069
R-Square	.356						
F-Test	16.770				0.000		

*p<.1, **p<.05, ***p<01.

5. Discussion

5.1 Theoretical implications

Over the past years, rapid developments on the Internet gave a whole other dimension to online privacy (Barth et al., 2019). The automatic gathering of online data from Internet users keeps on expanding and raises discussions about the opportunities and threats of these processes. Even though Internet users have access to loads of online information, the consequence is that situations could happen where personal information is being disclosed on online public spheres (Berners-Lee et al., 2001; Cumbley & Church, 2013; Hashem et al., 2015). These data breach situations can be framed as a corporate crisis and have a severe impact on public's perception on the organization in crisis. This research has its foundation in the Situational Crisis Communication Theory, which states that the greater the level of responsibility that is attributed to an organization, the higher the reputational damage on an organization, which subsequently affects the perceptions of the organization's stakeholders (Coombs, 2007). To decrease this damage, organizations try to use a proper crisis response strategy in which its effectiveness depends on the situation. Also, the power of pre-crisis reputation has an effect on the perceptions on organizations since a high pre-crisis reputation of an organization blocks negativities that can occur after the situation of a data breach crisis (Coombs & Holladay, 2006). On top of that, research done by Coombs (2007) and Wang and Wanjek (2018) has found that emotions like anger and sympathy are connected to the perceptions on organizations in crisis and secondary crisis communication. Also, the individual privacy concerns of stakeholders, before the crisis occurs, can have an impact. More specifically, previous research implied that privacy concerns can be seen as a negative tendency, which means that the more uncomfortable stakeholders are about privacy issues, the stronger the effects on weakening the perception on organizations (Motiwalla et al., 2014). Besides, the personal suggestion of the researcher suggested that a high privacy concern increased the amount of secondary crisis communication, since privacy concern can be seen as a negative tendency.

Although many academics had highlighted the importance of online privacy issues and their effect on stakeholders, a few studies focused on data breaches and did in-depth research on this relatively new subject (Alemany et al., 2019; Barth & de Jong, 2017; Winder, 2019). Most notably, in crisis communication research, most focus lies on investigating the most beneficial response strategies, and little is known about the perceptions of stakeholders (Kim, 2019). To address this audience-centered gap in the existing literature, an experimental research design with twelve conditions focused on different variables measured the impact on the perception on organizations in crisis, namely three types of data breach crises derived from the research of Confente et al (2019), two crisis response strategies and two emotions derived from Coomb's SCCT model (2007), individual privacy concern levels from the research of Motiwalla et al (2014) and organizations that represent a high and a low pre-crisis reputation (*N* = 563). In addition to that, the impact of emotion and individual privacy concerns on secondary crisis communication were included in this study. In this research, no significant effect was found of data breach crisis, response strategy, and privacy concern on the perception on organizations. However, this research did find validation that pre-crisis reputation and emotion had a significant effect on the perception on organizations. Besides, a significant effect was found of emotion and privacy concern on secondary crisis communication. Hypotheses were constructed to test the impact of these different variables and will be mentioned below, together with additional findings, concerning the analyses and associated results.

H1: Data breach crisis & perception on organizations

The study of Confente et al was used for the classification of data breach crises (2019). The recommendations made in this research about the impact of data breach crises on corporate reputation dimensions indicate that only in the case of intentional and internal data breaches, the valence was positive concerning comments from users after a data breach occurs. In contrast, unintentional and internal data breaches as well as intentional and external data breaches generate a negative valence regarding comments originating from users (Confente et al., 2019). This study's design relatively

questioned these outcomes as it investigated the impact of data breach crises on the perception on organizations instead of social media comments.

This study hypothesized that intentional and internal data breach crises would have a stronger impact on weakening the perception on organizations than unintentional and internal data breaches as well as intentional and external data breaches. Besides, unintentional and internal data breaches would have a stronger impact on weakening the perception on organizations than intentional and external data breaches. The results of this study identified an intentional and internal data breach crisis that did not have a stronger impact on weakening the perception on organizations than an unintentional and internal data breach crisis. Nevertheless, the results did demonstrate that an intentional and internal data breach crisis had a stronger impact on weakening the perception on organizations than an intentional and external data breach crisis. Therefore, this study partly rejects and partly accepts the first H1a. Also, this study rejects H1b since an unintentional and internal data breach crisis did not have a stronger impact on weakening the perception on organizations than an intentional and external data breach crisis.

For that reason, it has become clear that the perception on organizations situated in a data breach crisis would not change whether it took place with an intentional or an unintentional purpose. This finding is noteworthy since previous research suggests that unintentional events lead to less attribution of organizational blame and responsibility compared to intentional events. Intentional events lead to more attribution of organizational blame, which creates a worse perception on organizations (Cho & Gower, 2006; Coombs, 2007; Kim, 2016). The difference in the outcomes of previous research and this study could be explained by the fact that this study focused on data breach crises and not on crises in general.

However, the perception on organizations situated in a data breach crisis would change by the reason whether it happened on an internal or external ground since an internal data breach crisis created a weaker perception on organizations than an external data breach crisis. This finding was especially interesting since the study of Confente et al about the impact of data breach crises on corporate reputation dimensions indicates that only intentional and internal data breaches generate positive

comments stemming from users (2019). However, a crisis cause that is considered to be internal is often viewed as controllable. Likewise, a crisis cause that is considered to be external if often viewed as uncontrollable. Controllability of a crisis could be connected to the public's judgement of the organization as having more responsibility for the crisis, which forms a more negative impression of the organization (Lee, 2004).

H2: Crisis response strategies & perception on organizations

Moreover, a great extent of research has been conducted in the field of crisis response strategies. Many of those studies support that denial is the most effective crisis response strategy protecting an organization's reputation (Kim & Sung, 2014). However, much criticism has resulted on crisis managers who did choose to utilize the denial response strategy after a crisis (Coombs, Holladay & Claeys, 2016). In the victim cluster, in this study demonstrated as the intentional and external conditions, denial is the most suitable response strategy and even a better strategy than the no response strategy (Coombs, 2007; Coombs, 2006; Holladay & Claeys, 2016). In general, the most harmful response to any crisis is the no response strategy (Coombs, 2006).

Therefore, this research hypothesized that, within all three types of data breach crises, no response strategy had a stronger impact on weakening the perception on organizations than a denial response strategy. These hypotheses were all rejected, since the outcomes of our study revealed that, within all three types of data breach crisis, there was no difference in perception on an organization whether this organization uses a denial or a no response strategy.

For the internal and external conditions, the insignificance of the difference between the two response strategies could be explained, regardless of crisis type, by the fact that organizations are judged to be more responsible and blameworthy for the crisis when the organization tries to deny crisis responsibility (Lee, 2004). Also, the study of Coombs et al on the effects of crisis response strategy reveal that denial response strategy and silence will have a stronger impact on weakening the perception of stakeholders on the organization when this organization is found guilty, in other words in the intentional and internal and the unintentional and internal conditions (2016). Therefore, highly perceived crisis responsibilities and determinations of guilt are

indicators of the effectiveness of using a denial response strategy or a no response strategy. Alternatively stated, when an organization is responsible for a crisis, silence and denial are both ineffective response strategies, which explains why there is no difference in impact on the perception on organization (Coombs et al., 2016; Kim et al., 2004). This mentioned literature and the results of this study indicate that using the right crisis response strategy depends on every individual situation and could therefore warrant future research. This confirms that assuming uniformity in the decision on a 'best practice' for crisis communication is not feasible, and every crisis should be treated individually (Coombs, 2015)

H3: Pre-crisis reputation & perception on organizations

The next variable, namely the pre-crisis reputation of an organization, is discussed in much literature who share the same thoughts about the impact of this factor (Claeys & Cauberghe, 2015; Coombs & Holladay, 2006; Turk, Jin, Stewart & Hipple, 2012). Existing literature states that organizations with a favorable pre-crisis reputation withstand not as many reputational loss from a crisis since customers are hesitant to change their attitudes towards organizations, which results in the attributions of fewer crisis responsibilities.

The hypotheses of this research assumed that, within all of the three types of data breach crisis, a low pre-crisis reputation had a stronger impact on weakening the perception on organizations compared to a low pre-crisis reputation, which was found to be confirmed. Therefore, the third group of hypotheses were being accepted, which supports the existing literature on pre-crisis reputation. This research could verify that a high pre-crisis reputation is a critical factor in minimizing adverse effects of a data breach crisis because it indeed protected against the deterioration of the perception on organizations in crisis.

H4: Emotion, perception on organizations and secondary crisis communication

Furthermore, the SCCT model suggests that emotion plays a vital role in the behavioral responses of stakeholders after a crisis (Coombs, 2007). More anger occurs when attributions of crisis responsibilities increase, and sympathy occurs when there

are no responsibility judgments since, in this case, organizations are being seen as victims. These emotions may support or deny the effectiveness of different crisis response strategies (Coombs & Holladay, 2005; Jin, 2014).

This research hypothesized that, whether which type of data breach crisis occurs, more anger would have a stronger impact on weakening the perception on organizations and increased secondary crisis communication. Also, more sympathy would have a stronger impact on strengthening the perception on organizations and increased secondary crisis communication. The analyses of these fourth hypotheses gave significant results, so they could be accepted. These findings were in line with previous research stating that emotions in a crisis impact people's perceptions on the reputation of an organization and secondary crisis communication (Choi & Lin, 2009; Jin, Pang & Cameron, 2007; Wang & Wanjek, 2018). To specify, the importance of emotions lies in the extremes, which means that the more reliable the feelings of anger or sympathy, the easier for an organization to provoke negative feelings or supportive reactions from stakeholders (Coombs & Holladay, 2005; Wang & Wanjek, 2018).

H5: Individual privacy concern, perception on organizations and secondary crisis communication

As a final point, some existing literature address the occurrence of individual privacy concern, due to present digitalization practices (Dinev & Hart, 2006; Malhotra et al., 2004; Motiwalla et al., 2014). This privacy concern is growing, which has become apparent when research stated that individuals are getting more uncomfortable with companies who trade, share, and sell personal online information to other companies they engage with. This statement is primarily facilitated by the growing amount of news stories that report about data breaches. These news reports result in individuals' awareness about the occurrence of data breach crises and the increase of complaints about crises (Antón, Earp & Young, 2010).

This study hypothesized that, when there is a data breach crisis, a high individual privacy concern would have a stronger impact on weakening the perception on organizations but a higher impact on secondary crisis communication than a low

individual privacy concern. Privacy concern has a negative tendency because privacy fundamentalists, who have the most serious privacy concern, have trust issues towards organizations (Motiwalla et al., 2014). However, the results of this study indicated that individual privacy concerns did not have a stronger impact on weakening the perception on organizations situated in a data breach crisis. In contrast, the results of this study indicated that individual privacy concerns did have a higher impact on secondary crisis communication. These results addressed a gap in the literature between perception and behavior intentions caused by individual privacy concerns.

Other findings

Some other effects were found while conducting this research. Corporate crisis responsibility, which could also be described as attributions or the level of guilt defined by the participant about the organization in crisis, had an impact on the perception on organizations. The core conclusion was that the more perceived corporate crisis responsibility to be ascribed to an organization, the stronger the effects of a crisis on weakening the perception on organizations. This supported the SCCT model, which claims that a higher attribution towards an organization results in a higher reputational threat for the reputation of an organization after the occurrence of a crisis (Coombs, 2007).

Other findings of this research were that pre-crisis reputation, perception on organizations, corporate crisis responsibility, and age are significant predictors of secondary crisis communication. A high pre-crisis reputation of an organization resulted in more secondary crisis communication on that organization. Furthermore, the higher the perception on organizations, the higher the amount of secondary crisis communication. On top of that, the more corporate crisis responsibilities to be ascribed to an organization, the lower the intentions of secondary crisis communication. Also, the older the participants, the less likely to participate in secondary crisis communications.

5.2 Managerial implications

Due to digitalization, the relationship between businesses and their customers changed massively. Businesses can collect considerable amounts of personal data on

the Semantic Web to improve their online activities. Consequently, this personal information can be exposed to the public, which results in a data breach crisis (Cumbley & Church, 2013). When newspapers report about these data breach crises, the public frames their perception to these kinds of crises and engage in secondary crisis communication, which can have a low impact on the reputation of the organization. Therefore, crisis managers must find the best way to minimize the damage to the reputation of their organizations (Wang & Park, 2017). This research presents some managerial implications that must be taken into consideration.

First of all, crisis managers need to recognize the type of crisis their organization is situated in. In this way, they could manage the situation in the most beneficial way. Different data breach crises have various effects on the perception on organizations since this research states that mainly internal and external data breaches make the difference in those perceptions. Considering that internal data breach crises cause a more unfavorable perception on organizations, managers need to find a way to prevent these kinds of crises happening in an organization. The recognition of internal data breaches is very challenging because these data breaches involve people with legitimate access to internal resources and data. With the availability of highly technical tools, insiders can make their data breach actions challenging to detect. In this Big Data era, insiders are being revealed to more and more sensitive data. It is therefore essential for crisis managers to be aware of the considerable security challenges their organization is facing nowadays (Cheng, Liu & Yao, 2017).

It is also crucial for managers to be aware of their pre-crisis reputation. Maintaining a positive reputation before a crisis is a severe factor in minimizing the harmful effects of corporate crises, conducted through the ‘Halo-effect’ that works as a shield. Therefore, it is also vital for managers working at a low pre-crisis reputation organization to increase their pre-crisis reputation. A high pre-crisis reputation not only protects an organization from threats after a crisis but also creates advantages for organizations not situated in a crisis (van Riel & Fombrun, 2007, ch. 2). For that reason, managers should build reputational capital and an organization-stakeholder relationship by having positive interactions and communications with their stakeholders. At some

point, managers need to spend that reputational capital to help an organization to survive a corporate crisis (Coombs & Holladay, 2006).

Next, it is important for crisis managers to keep the emotion of their stakeholders in mind. If a stakeholder has anger towards an organization, it will undoubtedly have a stronger impact on weakening their perception on that organization, resulting in secondary crisis communications with a negative loading. On the other hand, when a stakeholder has sympathy towards an organization, this will result in a stronger impact on strengthening their perception towards that organization, resulting in secondary crisis communications with a positive loading. Anger is always related to the attribution of responsibility to the organization and includes the action of blame. These findings support why crisis managers' best practice is to react to stakeholders' angry expectations by taking a clear organizational position against the situation and delivering any just cause to blame (Jin, 2014). Strong sympathy could be handled best by crisis managers by ensuring that the organization acts as an action-facilitator to lead the public on how to take useful steps and leave the current crisis properly (Jin, 2014).

As a final point, even though individual privacy concern does not have a stronger impact on weakening the perception on organizations situated in a data breach crisis, it does increase the engagement of stakeholders in secondary crisis communication after the crisis. Therefore, crisis managers must have a grip on these individual privacy concerns. The digitalization of businesses raises these privacy concerns of individuals, which results in negative consumer responses and should require urgent attention from the management team of an organization (Wirtz, Lwin & Williams, 2007). Managers should effectively reduce privacy concerns, which can be realized by paying attention to business policies to enhance privacy protection. When managers start paying attention to web-based technologies' regulatory aspects and improve their organization's privacy policies, privacy concerns will reduce in the long run (Wirtz et al., 2007).

6. Conclusion

6.1 Summary of findings

The evolution of the Semantic Web questions how companies should handle their data gathering practices. These data gathering practices raise many privacy issues that could result in data breach crises that are being framed in, for instance, newspaper articles (Confente et al., 2019; Coombs, 2007). This experiment contributed to the field of crisis communication and management by creating an audience-centered focus on the effects of data breach crises, crisis communication strategy, pre-crisis reputation, individual privacy concern, and emotion on perception on organizations situated in a crisis. Besides, the effect of individual privacy concern and emotion on secondary crisis communication was also included. The study was established to understand how the perceptions of stakeholders were constructed after being exposed to a data breach crisis and if they were engaged in secondary crisis communication. This study was implemented to generate an answer to the following research questions: *How do crisis type (intentional and internal vs. unintentional and internal vs. intentional and external), crisis response strategy (denial vs. no response) and pre-crisis reputation (high vs. low) affect the perception on organizations after a data breach crisis?,* and *What are the roles of emotion and individual privacy concerns on perception on organizations and secondary crisis communication?.* Five hypotheses were determined to answer these research questions. To test these hypotheses, an online experiment was conducted using the online survey tool Qualtrics in combination with the online crowdsourcing platform Amazon Mechanical Turk. The final sample consisted of N = 563 participants. The experiment was situated around a fictitious online newspaper about either a high pre-crisis reputation organization or a low pre-crisis reputation organization, positioned in a data breach crisis and conducting a crisis response strategy. The high pre-crisis organization was Google, and the low pre-crisis organization was the fictitious brand SearchLand. These organizations were situated in an intentional and internal data breach, an unintentional and internal data breach, or an intentional and external data breach. The organization could respond with the denial response strategy or with the no response strategy. Participants of the experiment were randomly assigned to one of the

twelve conditions that represented one of the three data breach crises, one of the two pre-crisis reputation organizations and one of the two crisis response strategies.

Focusing on existing literature, this study expected a relationship between the independent variables of data breach crisis, crisis response strategy, pre-crisis reputation, individual privacy concern, and emotion and the dependent variable of perception on organizations. Also, a relationship between the independent variables of emotion and individual privacy concern and the dependent variable of secondary crisis communication was expected in this study. The results of this study supported some of these predictions and also rejected some of them. When a data breach crisis happened intentionally, an internal data breach had a stronger impact on weakening the perception on organizations than an external data breach. Also, results showed that, within all three types of data breach crises, a low pre-crisis reputation and more anger had a strong impact on weakening the perception on organizations. Besides, more sympathy had a strong impact on strengthening the perception on organizations. Resulting from that, more anger and sympathy had a stronger impact on secondary crisis communication. On the other hand, the results indicated that within an internal data breach, intentional data breaches did not have a stronger impact on weakening the perception on organizations than unintentional data breaches. Furthermore, unintentional and internal data breaches did not have a stronger impact on weakening the perception on organizations than intentional and external data breaches. Another rejection is that, within all three types of data breach crises, there was no impact on the perception on organizations whether these organization conducted a denial or no response communication strategy. There was also no impact on perception on organization on behalf of stakeholders' individual privacy concerns. Despite that, high individual privacy concerns did have a strong impact on secondary crisis communication.

To summarize, there are still some controversies in the academic field about what type of data breach crisis and crisis response strategy will result in the least harm on the perception on organizations and the role of individual privacy concerns in that context. At least it can be concluded that, within all three types of data breach crises, a high pre-crisis reputation and sympathy guarantee for a better perception on

organizations. Furthermore, strong anger, strong sympathy, and high individual privacy concerns raise engagement in secondary crisis communication. In this way, this research reconfirmed existing literature and has addressed an audience-centered gap in the academic field on crisis communication.

6.2 Limitations and directions for further research

After conducting this research and reviewing the whole progress, some limitations, and additional directions for further research will be discussed in this section. The first limitation is the scope of this research. The sampling for this research is conducted by convenience sampling by using the crowdsourcing platform Amazon Mechanical Turk to obtain a diverse and representative sample. The related dataset showed that most participants had a higher education, which meant they are in possession of either a bachelor's or master's degree. Nevertheless, examples of the data breach crises that were used in the fictitious newspaper articles are, in general, not limited to the higher educated part of the global population. Moreover, it has to be noted that the subject of data breach crises has global relevance, but it could be interpreted differently in different societies. The participants of this study came from a wide variety of nationalities and cultures, but there was a tilted situation towards participants with American and Indian nationalities. Hence, the response diversity was somewhat out of balance, which could have a restriction on the generalizability of the results. Therefore, for further research, this study recommends focusing on these specific regions to rationalize the cultural factors that could affect the perception on organizations in data breach crises and using a random sampling method to symbolize a more educational diverse population.

Second, based on the manipulation check of crisis response strategies, the percentage of the participants that passed the manipulation of recognizing the denial response strategy was somewhat low (69.5%), despite that the manipulation check test demonstrated that the crisis response strategy variable succeeded the manipulation. The sentence at the end of the newspaper article in the denial response conditions saying *'... is unclear due to the fact that Google/SearchLand denies the existence of this data breach accident'* did not display a very obvious denotation of the fact that the

organization provided a denial response strategy. This low percentage could be explained by the fact that this manipulation was not presented in the newspaper article heading, which allowed some participants to miss the manipulation. This manipulation should have been clarified more in the newspaper articles to increase the reliability of the results related to this manipulation.

Third, this study focused on the investigation of the participants' perception, based only on the short textual content of data breach crises by using online newspaper articles. Nonetheless, data breach crises could exist in other additional forms like reactions on social media or other news sources like television and radio programs. A crisis often breaks, for instance, on Twitter and leads to the reporting on traditional media afterwards. This multichannel approach creates a more complete image of the exact occurrence of the crisis (Syed, 2019; Sung & Hwang, 2014). These mentioned indications could also have an impact on the perception on organizations in a data breach crisis. This resulted in the disadvantage that the focus of this study on solely textual content, which consists of a short description of the crisis, could potentially limit the generalizability of the findings.

Furthermore, for the low pre-crisis reputation organization, this study used a fictitious brand named SearchLand to exclude any prior bias in the form of an already existing favorable opinion towards the organization. This decision meant that participants in this study generalized their opinions on this organization purely on the information that was exposed in the online newspaper article. Hence, in real-life, these data breach crises happen at already existing organizations that already have a pre-crisis reputation at any level based on their crisis history. Further research could potentially use an already existing organization that has a low pre-crisis reputation to generate some different outcomes of the results. To test if the participants perceive this organization as an owner of a low pre-crisis reputation, a comprehensive pre-test must be conducted.

Another limitation was the fact that this experimental design could be further improved since it only used two different response strategies, namely a denial, and a no response strategy. Further research could have the advantage of a more extensive experiment that includes all of the response strategies of the SCCT model by Coombs

because these strategies could also potentially have a statistically significant relationship with the variable of perception on organizations (2007).

This study also found that the effect of a data breach crisis had an almost significant impact on the perception on organizations. Due to the contiguity to a significant level and the outcome of the post hoc tests that partly showed a significant effect between an intentional and internal data breach crisis and an intentional and external data breach crisis, further research could explore the impact of data breach crises and the perception on organizations conceivably in a different research design.

Ideally, it would be beneficial if future research investigates the perception on organizations after a data breach crisis over time. This research was only based on a glance of the occurring perceptions of the participants. These perceptions could increase or decrease after a crisis since the possibility exists that the participants could either put their opinions down or reinforce these opinions if they had more time to think about it. Further research could be a longitudinal study that presents a survey at different times to investigate public opinion in a developing progress.

Other recommendations for future research are an investigation into the relationship between corporate crisis responsibilities and the perception on organizations, why there are differences in the impact on perception on organizations between intentional and unintentional data breaches that happen internally, and the relationship between the variables pre-crisis reputation of Google, perception on organizations, corporate crisis responsibilities and the demographic factor of age as predictors of secondary crisis communication. Another addition to further research could be to extend this research by also investigating the effect of crisis type, pre-crisis reputation and crisis response strategy on secondary crisis communication in the context of a data breach crisis since this study only focused on the impact of emotion and individual privacy concern on secondary crisis communication. These additional findings offer an interesting approach of opportunities in the academic field to fill other gaps in the literature by generalizing the effects regarding these variables.

References

Acquisti, A. & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3(1),* 26-33.

Alemany, J., Val, del, E., Alberola, J. & García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human-Computer Studies, 129,* 27-40.

Antón, A. I., Earp, J. B. & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy, 8(1),* 21-27.

Aula, P. (2010). Social media, reputation risk and ambient publicity management. *Strategy & Leadership, 38(6),* 43-49.

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.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49(2),* 138-150.

Barth, S. & De Jong, M. D. T. (2017). The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and Informatics, 34(7),* 1038-1058.

Barth, S., De Jong, M. D. T., Junger, M., Hartel, P. H. & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics, 41,* 55-69.

Becker, K. & Lee, J. W. (2019). Organizational Usage of Social Media for Corporate Reputation Management. *Journal of Asian Finance, Economics and Business, 6(1),* 231-240.

Berners-Lee, T., Hendler, J. & Lassila, O. (2001). The Semantic Web. *Scientific American*, 284(5), 34-43.

Boerman, S. C., van Reijmersdal, E. A. & Neijens, P. C. (2012). Sponsorship disclosure: Effects of duration on persuasion knowledge and brand responses. *Journal of Communication, 62(6),* 1047-1064.

Box, J. F. (1980). RA Fisher and the design of experiments, 1922-1926. *The American Statistician, 34(1),* 1-7.

Brown, B. (2001). Studying the internet experience. *HP Laboratories Technical Report HPL, 49.*

Buhrmester, M., Kwang, T. & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data?. *Perspectives on Psychological Science, 6(1),* 3-5.

Cheng, L., Liu, F. & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5),* 1-14.

Cho, S. H. & Gower, K. K. (2006). Framing effect on the public's response to crisis: Human interest frame and crisis type influencing responsibility and blame. *Public Relations Review, 32(4),* 420-422.

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.

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

Confente, I., Siciliano, G. G., Gaudenzi, B. & Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal, 37(4),* 492-504.

Coombs, W. T. (2004). Impact of past crises on current crisis communication insights from Situational Crisis Communication Theory. *Journal of Business Communication , 41(3),* 265-289.

Coombs, W. T. (2006). The protective powers of crisis response strategies: Managing reputational assets during a crisis. *Journal of Promotion Management, 12(3-4),* 241-260.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10(3),* 163-176.

Coombs, W. T. (2015). The value of communication during a crisis: Insights from strategic communication research. *Business Horizons, 58 (2)*, 141-148.

Coombs, W. T. & Holladay, S. J. (1996). Communication and attributions in a crisis: An experimental study in crisis communication. *Journal of Public Relations Research, 8(4),* 279-295.

Coombs, W. T. & Holladay, S. J. (2001). An extended examination of the crisis situations: A fusion of the relational management and symbolic approaches. *Journal of Public Relations Research, 13(4),* 321-340.

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

Coombs, W. T. & Holladay, S. J. (2005). An exploratory study of stakeholder emotions: affect and crises. *The Effect of Affect in Organizational Settings Research on Emotion in Organizations, 1(5),* 263-280.

Coombs, W. T. & Holladay, S. J. (2006). Unpacking the Halo Effect: Reputation and Crisis Management. *Journal of Communication Management, 10(2),* 123-137.

Coombs, W. T. & Holladay, S. J. (2011). An exploration of the effects of victim visuals on perceptions and reactions to crisis events. *Public Relations Review, 37(2),* 115-120.

Coombs, W. T., Holladay, S. J. & Claeys, A. (2016). Debunking the myth of denial's effectiveness in crisis communication: context matters. *Journal of Communication Management, 20(4),* 381-395.

Cooper, A. H. (2002). Media framing and social movement mobilization: German peace protest against INF missels, the Gulf War, and NATO peace enforcement is Bosnia. *European Journal of Political Research, 41(1),* 37-80.

Cumbley, R. & Church, P. (2013). Is "Big Data" creepy? *Computer Law & Security Review, 29(5),* 601-609.

Czarnecki, S. (2018, October 11). Study: Google has the best reputation for corporate responsibility in the world. *PR week.* Retrieved from https://www.prweek.com/article/1495753/study-google-best-reputation-corporate-responsibility-world.

Das, R. & Patel, M. (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. *International Journal for Research in Applied Science & Engineering Technology, 5(4),* 833-838.

Davies, G. & Olmedo-Cifuentes, I. (2016). Corporate misconduct and the loss of trust. *European Journal of Marketing, 50(7/8),* 1426-1447.

Decker, W. H. (2012). A firm's image following alleged wrongdoing: Effects of the firm's prior reputation and response to the allegation. *Corporate Reputation Review, 15(1),* 20-34.

Dijkmans, C., Kerkhof, P. & Beukeboom, C. J. (2015). A stage to engage: Social media use and corporate reputation. *Tourism Management, 47,* 58-67.

Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17(1),* 61-80.

Druckman, J. N. (2001). The implications of framing effects for citizen competence. *Political Behavior, 23(3),* 225-256.

Flender, C., Müller, G. (2012). Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited. In *International Symposium on Quantum Interaction* (pp. 148-159). Springer, Berlin, Heidelberg.

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.

Graf, D., & Schwede, B. (2012, April 24). *Shitstorm-Skala: Wetterbericht für Social Media.* Retrieved from https://feinheit.ch/blog/shitstorm-skala/.

Griffin, M., Babin, B. J. & Darden, W. R. (1992). Consumer assessments of responsibility for product-related injuries: The impact of regulations, warnings, and promotional policies. *ACR North American Advances.*

Hajikazemi, S., Ekambaram, A., Andersen, B., & Zidane, Y. J. (2016). The black swan – knowing the unknown in projects. *Procedia - Social and Behavioral Sciences, 226*, 184-192.

Harris, L. & Westin, A. F. (1991). Harris-Equifax Consumer Privacy Survey 1991. Atlanta: Equifax Inc.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A. & Khan, S. U. (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information Systems, 47,* 98-115.

Jin, Y. (2014). Examining Public’s Crisis Responses According to Different Shades of Anger and Sympathy. *Journal of Public Relations Research, 26(1),* 79-101.

Jin, Y., Pang, A. & Cameron, G. T. (2007). Integrated crisis mapping: Towards a publics-based, emotion-driven conceptualization in crisis communication. *Sphera Publica, 7(1),* 79-101.

Kiambi, D. M. & Shafer, A. (2016). Corporate Crisis Communication: Examining the Interplay of Reputation and Crisis Response Strategies. *Mass Communication and Society, 19(2),* 127-148.

Kim, J. (2019). Underlying processes of SCCT: Mediating roles of preventability, blame, and trust. *Public Relations Review, 45(3),* 1-8.

Kim, Y. (2016). Understanding publics’ perception and behaviors in crisis communication: Effects of crisis news framing and publics’ acquisition, selection, and transmission of information in crisis situations. *Journal of Public Relations Research, 28(1),* 35-60.

Kim, S. & Sung, K.H. (2014). Revisiting the effectiveness of base crisis response strategies in comparison of reputation management crisis responses. *Journal of Public Relations Research, 26(1),* 62-78.

Kohler, T. & Chesbrough, H. (2019). From collaborative community to competitive market: the quest to build a crowdsourcing platform for social innovation. *R&D Management, 49(3),* 356-368.

Lee, B. K. (2004). Audience-oriented approach to crisis communication. A study of Hong Kong consumers' evaluation of an organizational crisis. *Communication research, 31(5),* 600-618.

Lowry, P. B., D'Arcy, J., Hammer, B. & Moody, G. D. (2016). "Cargo Cult' science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems, 25(3),* 232-240.

McDonald, L., Glendon, A. I., & Sparks, B. (2011). Measuring Consumers' Emotional Reactions to Company Crises: Scale Development and Implications. *Advances in Consumer Research, 39,* 333-340.

Maal, M. & Wilson-North, M. (2019). Social media in crisis communication – the "do's" and "don'ts". *International Journal of Disaster Resilience in the Built Environment*, *10(5)*, 379-391.

Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15(4),* 336-355.

Mangold, W. G. & Faulds, D. J. (2009). Social media: The new hybrid element of the promotion mix. *Business Horizons, 52(4),* 357-365.

Motiwalla, L. F., Li, X. & Liu, X. (2014, June). Privacy Paradox: Does Stated Privacy Concerns Translate into the Valuation of Personal Information?. *Pacific Asia Conference on Information Systems (PACIS)* (p. 281).

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches.* Essex, UK: Pearson Education.

Ott, L., & Theunissen, P. (2015). Reputations at risk: Engagement during social media crisis. *Public Relations Review, 41(1),* 97-102.

Pallant, J. (2014). *SPSS Survival Manual.* (5th ed.). Maidenhead, UK: McGraw-Hill.

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.

Pötzsch, S. (2008, September). Privacy awareness: A means to solve the privacy paradox? In *IFIP Summer School on the Future of Identity in the Information Society* (p. 226-236). Springer, Berlin, Heidelberg.

Prpic, J., Shukla, P. P., Kietzmann, J. H. & McCarthy, I. P. (2015). How to work a crowd: Developing crowd capital through crowdsourcing. *Business Horizons, 58(1),* 77-85.

Riel, van, C. B. & Fombrun, C. J. (2007). *Essentials of corporate communication: Implementing practices for effective reputation management.* London: Routledge.

Ross, J., Irani, L., Silberman, M. S., Zaldivar, A. & Tomlinson, B. (2010, April 14). Who are the crowdworkers? Shifting demographics in Mechanical Turk. *Proceedings of the 28th Annual CHI Conference on Human factors in Computing Systems,* 2863-2872.

Schultz, F., Utz, S., & Goöritz, 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.

Seeger, M. W., Sellnow, T. L. & Ulmer, R. R. (2003). *Communication and Organizational Crisis.* Westport: Greenwood Publishing Group.

Selm, van, M. & Jankowski, N. W. (2006). Conducting online surveys. *Quality and Quantity, 40(3),* 435-456.

Sen, R. & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32(2),* 314-341.

Shank, D. B. (2015). Using Crowdsourcing Websites for Sociological Research: The Case of Amazon Mechanical Turk. *The American Sociologist, 47(1),* 47-55.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: An inter-disciplinary review. *MIS Quarterly, 35,* 989-1015.

Sung, M. & Hwang, J. (2014). Who drives a crisis? The diffusion of an issue through social networks. *Computers in Human Behavior, 36,* 246-257.

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *Journal of Strategic Information Systems, 28(3),* 257-274.

Taddicken, M. (2010). *Measuring Online Privacy Concern and Protection in the (Social) Web: Development of the APCP and APCP-18 Scale.* [Paper presentation]. 60th Annual Conference of the International Communication Association, Singapore.

Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication, 19(2),* 248-273.

Turk J. V., Jin, Y., Stewart, S., Kim, J. & Hipple, J. R. (2012). Examining the interplay of an organization's prior reputation, CEO's visibility, and immediate response to a crisis. *Public Relations Review, 38(4),* 574-583.

Veil, S., Buehner, T. & Palenchar, M.J. (2011). A work-in-process literature review: incorporating social media in risk and crisis communication. *Journal of Contingencies and Crisis Management, 19(2),* 110-122.

Wang, T., Duong, T. D. & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36(4),* 531-542.

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.

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.

Watson, A. (2019). Credibility of the New York Times in the U.S. 2019. *Statista.* Retrieved from https://www.statista.com/statistics/239749/credibility-of-the-new-york-times-in-the-united-states/.

Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychology Review, 92(4),* 548-573.

Weiner, B. (1986). *An Attributional Theory of Motivation and Emotion,* Springer Verlag, New York.

Weiner, B. (2006). *Social Motivation, Justice, and the Moral Emotions: An Attributional Approach,* Lawrence Erlbaum Associates, Inc., Mahwah, NJ.

Winder, D. (2019). Data Breaches Expose 4.1 Billion Records in First Six Months of 2019. *Forbes.* Retrieved from https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/.

Wirtz, J., Lwin, M. O. & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18(4),* 326-348.

Wong, J. C. & Solon, O. (2018). Google to shut down Google+ after failing to disclose user data leak. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2018/oct/08/google-plus-security-breach-wall-street-journal.

Woon, E. & Pang, A. (2017). Explicating the information vacuum: stages, intensifications, and implications. *Corporate Communications: An International Journal, 22(3),* 329-253.

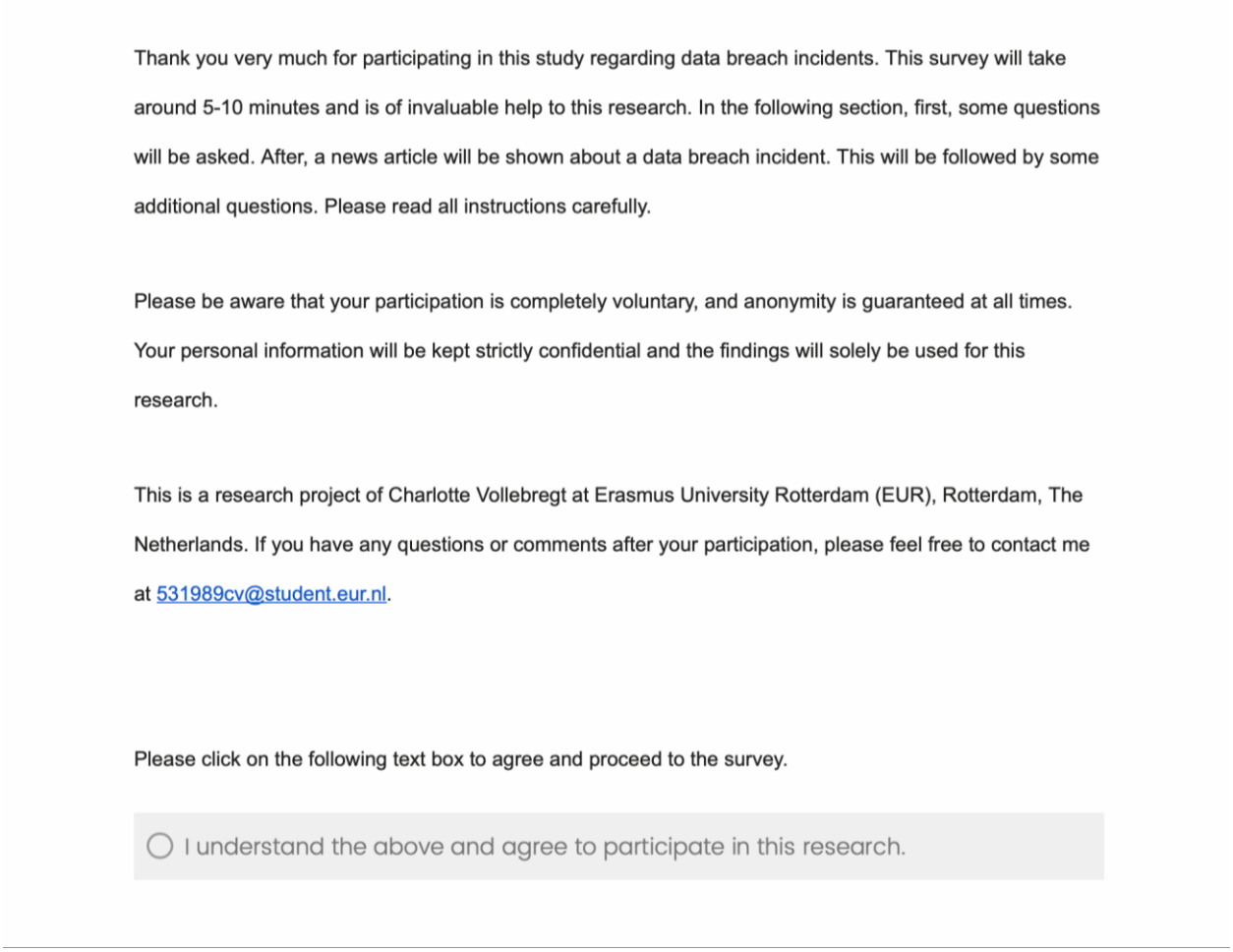
Yu, L., Li, H., He, W., Wang, F. & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management, 51,* 1-10.

Zheng, B., Liu, H., & Davison, R. M. (2018). Exploring the relationship between corporate reputation and the public's crisis communication on social media. *Public Relations Review, 44(1),* 56-64.

Zou, Y., Danino, S., Sun, K. & Schaub, F. (2019, May 4-9). *You 'Might' Be Affected: An Emperical Analysis of Readability and Usability Issues in Data Breach Notifications.* [Paper presentation]. CHI Conference on Human Factors in Computing Systems Proceedings, Glasgow, Scotland UK.

Appendix A - Online experiment including stimulus material

A.1 - Introduction and informed consent



Thank you very much for participating in this study regarding data breach incidents. This survey will take around 5-10 minutes and is of invaluable help to this research. In the following section, first, some questions will be asked. After, a news article will be shown about a data breach incident. This will be followed by some additional questions. Please read all instructions carefully.

Please be aware that your participation is completely voluntary, and anonymity is guaranteed at all times. Your personal information will be kept strictly confidential and the findings will solely be used for this research.

This is a research project of Charlotte Vollebregt at Erasmus University Rotterdam (EUR), Rotterdam, The Netherlands. If you have any questions or comments after your participation, please feel free to contact me at 531989cv@student.eur.nl.

Please click on the following text box to agree and proceed to the survey.

◯ I understand the above and agree to participate in this research.

Figure A.1.1 Screenshot of introduction and consent

A.2 Questions measuring individual privacy concern

Please answer the following questions about privacy using the full scale provided.

In general, how concerned are you about your privacy while using the Internet?

- ○ Not at all
- ○ Slightly
- ○ Moderately
- ○ Very
- ○ Extremely

Are you concerned that you are asked for too much personal information when you register or make online purchases?

- ○ Not at all
- ○ Slightly
- ○ Moderately
- ○ Very
- ○ Extremely

Figure A.2.1 Screenshot of items measuring individual privacy concern

A.3 Manipulation check questions for high pre-crisis reputation conditions (1, 2, 3, 7, 8, and 9)

Please answer the following questions about Google.

Do you know Google?

- ◯ Yes
- ◯ No

Google is a company I have a good feeling about.

- ◯ Strongly Disagree
- ◯ Disagree
- ◯ More Or Less Disagree
- ◯ Undecided
- ◯ More Or Less Agree
- ◯ Agree
- ◯ Strongly agree

Google is a company that I trust.

- ◯ Strongly Disagree
- ◯ Disagree
- ◯ More Or Less Disagree
- ◯ Undecided
- ◯ More Or Less Agree
- ◯ Agree
- ◯ Strongly agree

Google is a company that I admire and respect.

- ◯ Strongly Disagree
- ◯ Disagree
- ◯ More Or Less Disagree
- ◯ Undecided
- ◯ More Or Less Agree
- ◯ Agree
- ◯ Strongly agree

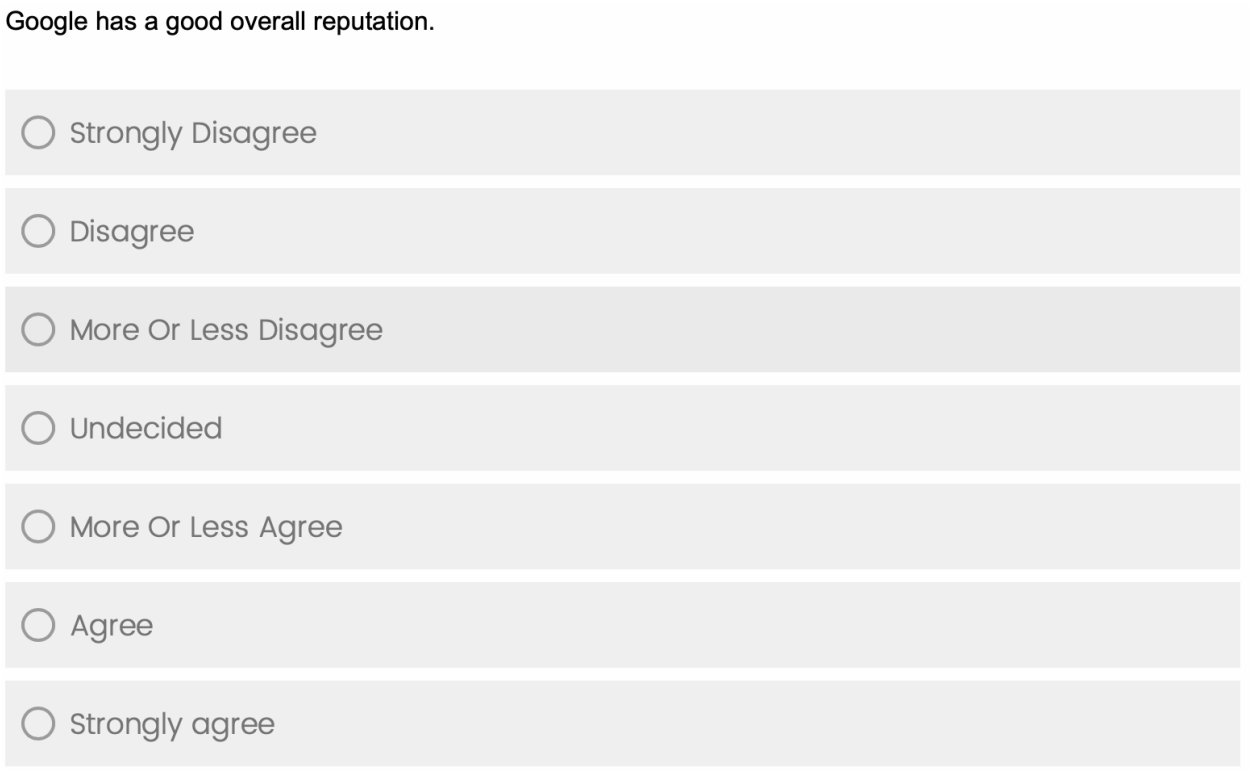


Figure A.3.1 Screenshot of manipulation check questions for the high pre-crisis reputation conditions

A.4 Manipulation check question for the low pre-crisis reputation conditions (4, 5, 6, 10, 11 and 12).

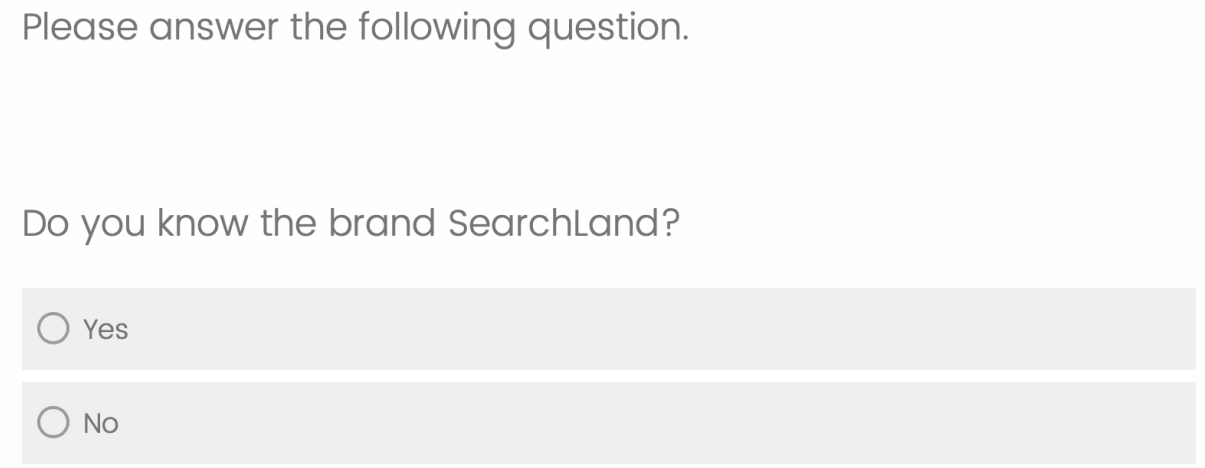


Figure A.4.1 Screenshot of manipulation check question for the low pre-crisis reputation conditions

A.5 Introduction stimulus material

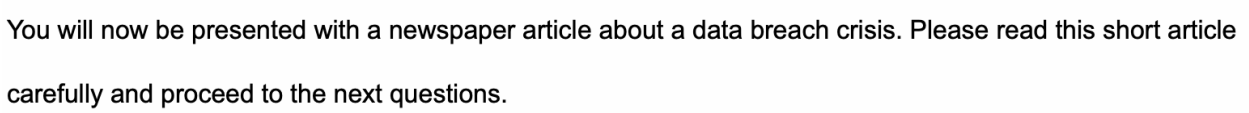
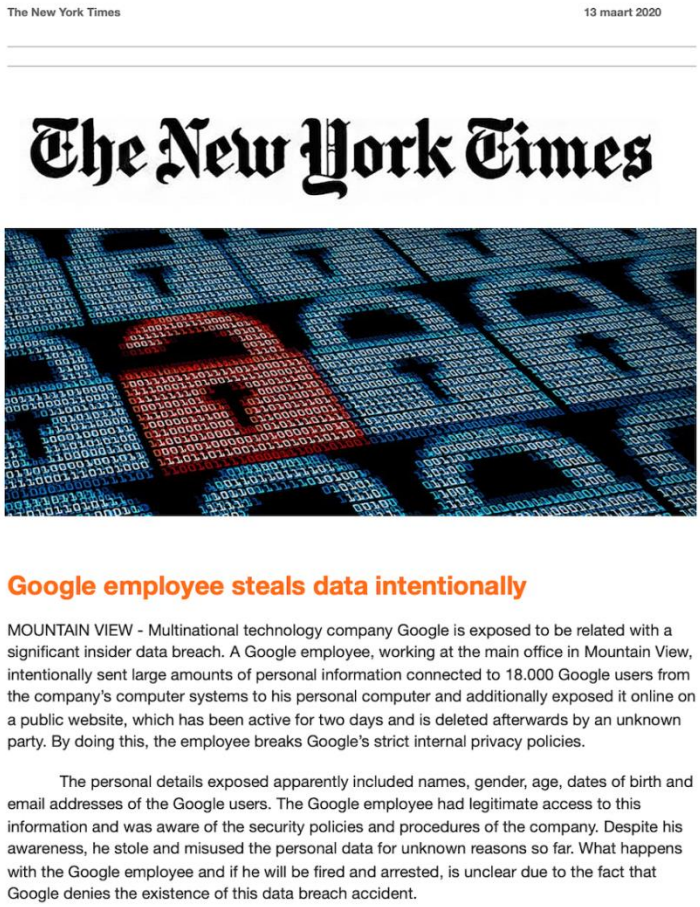


Figure A.5.1 Screenshot of introduction stimulus material

A.6 Stimulus material for the twelve experimental conditions



The New York Times 13 maart 2020

The New York Times

Google employee steals data intentionally

MOUNTAIN VIEW - Multinational technology company Google is exposed to be related with a significant insider data breach. A Google employee, working at the main office in Mountain View, intentionally sent large amounts of personal information connected to 18.000 Google users from the company's computer systems to his personal computer and additionally exposed it online on a public website, which has been active for two days and is deleted afterwards by an unknown party. By doing this, the employee breaks Google's strict internal privacy policies.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the Google users. The Google employee had legitimate access to this information and was aware of the security policies and procedures of the company. Despite his awareness, he stole and misused the personal data for unknown reasons so far. What happens with the Google employee and if he will be fired and arrested, is unclear due to the fact that Google denies the existence of this data breach accident.

Figure A.6.1 Screenshot of condition 1 - Intentional and internal / High pre-crisis reputation / Denial response strategy

The New York Times 13 maart 2020

The New York Times

Google employee accidentally discloses data

MOUNTAIN VIEW - Multinational technology company Google is exposed to be related with a data breach incident as a result of human error. Because of a Google employee, working at the main office in Mountain View, a cloud server including large amounts of personal information connected to 18.000 Google users left open to the public. This accident happened due to the fact that a cloud repository was misconfigured to allow public access.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the Google users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the database is no longer public and researchers are unable to determine whether anyone accessed the files. What happens with the Google employee and if he will be fired, is unclear due to the fact that Google denies the existence of this data breach accident.

Figure A.6.2 Screenshot of condition 2 - Unintentional and internal / High pre-crisis reputation / Denial response strategy

The New York Times 13 maart 2020

The New York Times

Google being hacked by outside party

MOUNTAIN VIEW - Multinational technology company Google is exposed to be related with a big hacking incident. A still anonymous group of hackers was able to enter the online system of Google and had access to great amounts of personal information. The attack compromised personal data connected to 18.000 Google users that was locked in the company's computer systems. The hacking group additionally exposed this information online on a public website, which has been active for two days and is deleted afterwards by an unknown party. Supposedly, this hacking incident has been conducted by using the robust bcrypt algorithm.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the Google users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the data is no longer public and researchers are unable to determine how many computers have accessed the files. What happens with Google's online protection systems, is unclear due to the fact that Google denies the existence of this data breach accident.

Figure A.6.3 Screenshot of condition 3 - Intentional and external / High pre-crisis reputation / Denial response strategy

The New York Times 13 maart 2020

The New York Times

SearchLand employee steals data intentionally

NEW YORK - Multinational technology company SearchLand is exposed to be related with a significant insider data breach. A SearchLand employee, working at the main office in New York, intentionally sent large amounts of personal information connected to 18.000 SearchLand users from the company's computer systems to his personal computer and additionally exposed it online on a public website, which has been active for two days and is deleted afterwards by an unknown party. By doing this, the employee breaks SearchLand's strict internal privacy policies.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the SearchLand users. The SearchLand employee had legitimate access to this information and was aware of the security policies and procedures of the company. Despite his awareness, he stole and misused the personal data for unknown reasons so far. What happens with the SearchLand employee and if he will be fired and arrested, is unclear due to the fact that SearchLand denies the existence of this data breach accident.

Figure A.6.4 Screenshot of condition 4 - Intentional and internal / Low pre-crisis reputation / Denial response strategy

The New York Times 13 maart 2020

The New York Times

SearchLand employee accidentally discloses data

NEW YORK - Multinational technology company SearchLand is exposed to be related with a data breach incident as a result of human error. Because of a Google employee, working at the main office in New York, a cloud server including large amounts of personal information connected to 18.000 SearchLand users left open to the public. This accident happened due to the fact that a cloud repository was misconfigured to allow public access.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the SearchLand users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the database is no longer public and researchers are unable to determine whether anyone accessed the files. What happens with the SearchLand employee and if he will be fired, is unclear due to the fact that SearchLand denies the existence of this data breach accident.

Figure A.6.5 Screenshot of condition 5 - Unintentional and internal / Low pre-crisis reputation / Denial response strategy

The New York Times 13 maart 2020

The New York Times

SearchLand being hacked by outside party

NEW YORK - Multinational technology company SearchLand is exposed to be related with a big hacking incident. A still anonymous group of hackers was able to enter the online system of SearchLand and had access to great amounts of personal information. The attack compromised personal data connected to 18.000 SearchLand users that was locked in the company's computer systems. The hacking group additionally exposed this information online on a public website, which has been active for two days and is deleted afterwards by an unknown party. Supposedly, this hacking incident has been conducted by using the robust bcrypt algorithm.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the SearchLand users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the data is no longer public and researchers are unable to determine how many computers have accessed the files. What happens with SearchLand's online protection systems, is unclear due to the fact that SearchLand denies the existence of this data breach accident.

Figure A.6.6 Screenshot of condition 6 - Intentional and external / Low pre-crisis reputation / Denial response strategy

The New York Times 13 maart 2020

The New York Times

Google employee steals data intentionally

MOUNTAIN VIEW - Multinational technology company Google is exposed to be related with a significant insider data breach. A Google employee, working at the main office in Mountain View, intentionally sent large amounts of personal information connected to 18.000 Google users from the company's computer systems to his personal computer and additionally exposed it online on a public website, which has been active for two days and is deleted afterwards by an unknown party. By doing this, the employee breaks Google's strict internal privacy policies.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the Google users. The Google employee had legitimate access to this information and was aware of the security policies and procedures of the company. Despite his awareness, he stole and misused the personal data for unknown reasons so far. What happens with the Google employee and if he will be fired and arrested, is unclear due to the fact that Google refuses to respond to the data breach accident.

Figure A.6.7 Screenshot of condition 7 - Intentional and internal / High pre-crisis reputation / No response strategy

The New York Times 13 maart 2020

The New York Times

Google employee accidentally discloses data

MOUNTAIN VIEW - Multinational technology company Google is exposed to be related with a data breach incident as a result of human error. Because of a Google employee, working at the main office in Mountain View, a cloud server including large amounts of personal information connected to 18.000 Google users left open to the public. This accident happened due to the fact that a cloud repository was misconfigured to allow public access.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the Google users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the database is no longer public and researchers are unable to determine whether anyone accessed the files. What happens with the Google employee and if he will be fired and arrested, is unclear due to the fact that Google refuses to respond to the data breach accident.

Figure A.6.8 Screenshot of condition 8 - Unintentional and internal / High pre-crisis reputation / No response strategy

The New York Times 13 maart 2020

The New York Times

Google being hacked by outside party

MOUNTAIN VIEW - Multinational technology company Google is exposed to be related with a big hacking incident. A still anonymous group of hackers was able to enter the online system of Google and had access to great amounts of personal information. The attack compromised personal data connected to 18.000 Google users that was locked in the company's computer systems. The hacking group additionally exposed this information online on a public website, which has been active for two days and is deleted afterwards by an unknown party. Supposedly, this hacking incident has been conducted by using the robust bcrypt algorithm.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the Google users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the data is no longer public and researchers are unable to determine how many computers have accessed the files. What happens with Google's online protection systems, is unclear due to the fact that Google refuses to respond to the data breach accident.

Figure A.6.9 Screenshot of condition 9 - Intentional and external / High pre-crisis reputation / No response strategy

The New York Times 13 maart 2020

The New York Times

SearchLand employee steals data intentionally

NEW YORK - Multinational technology company SearchLand is exposed to be related with a significant insider data breach. A SearchLand employee, working at the main office in New York, intentionally sent large amounts of personal information connected to 18.000 SearchLand users from the company's computer systems to his personal computer and additionally exposed it online on a public website, which has been active for two days and is deleted afterwards by an unknown party. By doing this, the employee breaks SearchLand's strict internal privacy policies.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the SearchLand users. The SearchLand employee had legitimate access to this information and was aware of the security policies and procedures of the company. Despite his awareness, he stole and misused the personal data for unknown reasons so far. What happens with the SearchLand employee and if he will be fired and arrested, is unclear due to the fact that SearchLand refuses to respond to the data breach accident.

Figure A.6.10 Screenshot of condition 10 - Intentional and internal / Low pre-crisis reputation / No response strategy

The New York Times 13 maart 2020

The New York Times

SearchLand employee accidentally discloses data

NEW YORK - Multinational technology company SearchLand is exposed to be related with a data breach incident as a result of human error. Because of a Google employee, working at the main office in New York, a cloud server including large amounts of personal information connected to 18.000 SearchLand users left open to the public. This accident happened due to the fact that a cloud repository was misconfigured to allow public access.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the SearchLand users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the database is no longer public and researchers are unable to determine whether anyone accessed the files. What happens with the SearchLand employee and if he will be fired and arrested, is unclear due to the fact that SearchLand refuses to respond to the data breach accident.

Figure A.6.11 Screenshot of condition 11 - Unintentional and internal / Low pre-crisis reputation / No response strategy

The New York Times 13 maart 2020

The New York Times

SearchLand being hacked by outside party

NEW YORK - Multinational technology company SearchLand is exposed to be related with a big hacking incident. A still anonymous group of hackers was able to enter the online system of SearchLand and had access to great amounts of personal information. The attack compromised personal data connected to 18.000 SearchLand users that was locked in the company's computer systems. The hacking group additionally exposed this information online on a public website, which has been active for two days and is deleted afterwards by an unknown party. Supposedly, this hacking incident has been conducted by using the robust bcrypt algorithm.

The personal details exposed apparently included names, gender, age, dates of birth and email addresses of the SearchLand users, which were accessible for two days and could be downloaded from every personal computer. At this moment, the data is no longer public and researchers are unable to determine how many computers have accessed the files. What happens with SearchLand"s online protection systems, is unclear due to the fact that SearchLand refuses to respond to the data breach accident.

Figure A.6.12 Screenshot of condition 12 - Intentional and external / Low pre-crisis reputation / No response strategy

A.7 Questions measuring perception on organisations

Please indicate below your opinion based on the statement: “I associate the company in the newspaper article as…” using the following criteria.

I associate the company in the newspaper article as…

- ◯ Very Bad
- ◯ Bad
- ◯ Somewhat Bad
- ◯ Neutral
- ◯ Somewhat Good
- ◯ Good
- ◯ Very Good

I associate the company in the newspaper article as…

- ◯ Very Unpleasant
- ◯ Unpleasant
- ◯ Somewhat Unpleasant
- ◯ Neutral
- ◯ Somewhat Pleasant
- ◯ Pleasant
- ◯ Very Pleasant

I associate the company in the newspaper article as…

- ◯ Very Unfavorable
- ◯ Unfavorable
- ◯ Somewhat Unfavorable
- ◯ Neutral
- ◯ Somewhat Favorable
- ◯ Favorable
- ◯ Very Favorable

I associate the company in the newspaper article as…

- ◯ Very Negative
- ◯ Negative
- ◯ Somewhat Negative
- ◯ Neutral
- ◯ Somewhat Positive
- ◯ Positive
- ◯ Very Positive

I associate the company in the newspaper article as…

- ◯ Very Dislikeable
- ◯ Dislikeable
- ◯ Somewhat Dislikeable
- ◯ Neutral
- ◯ Somewhat Likeable
- ◯ Likeable
- ◯ Very Likeable

Figure A.7.1 Screenshot of items measuring perception on organisations

A.8 Questions measuring emotion

Figure A.8.1 Screenshot of items measuring emotion

A.9 Questions measuring corporate crisis responsibility

Please answer the following questions:

Circumstances, not the company, are responsible for the crisis.

- ○ Strongly Disagree
- ○ Disagree
- ○ More Or Less Disagree
- ○ Undecided
- ○ More Or Less Agree
- ○ Agree
- ○ Strongly Agree

The blame for the crisis lies with the company.

- ○ Strongly Disagree
- ○ Disagree
- ○ More Or Less Disagree
- ○ Undecided
- ○ More Or Less Agree
- ○ Agree
- ○ Strongly Agree

The blame for the crisis lies in the circumstances, not the company.

- ○ Strongly Disagree
- ○ Disagree
- ○ More Or Less Disagree
- ○ Undecided
- ○ More Or Less Agree
- ○ Agree
- ○ Strongly Agree

Figure A.9.1 Screenshot of items measuring corporate crisis responsibility

A.10 Questions measuring secondary crisis communication

Please answer the following questions:

I would like to share the news with other people.

- ○ Strongly Disagree
- ○ Disagree
- ○ More Or Less Disagree
- ○ Undecided
- ○ More Or Less Agree
- ○ Agree
- ○ Strongly Agree

I would like to tell my friends about the incident.

- ○ Strongly Disagree
- ○ Disagree
- ○ More Or Less Disagree
- ○ Undecided
- ○ More Or Less Agree
- ○ Agree
- ○ Strongly Agree

I would like to leave a reaction to this news.

- ○ Strongly Disagree
- ○ Disagree
- ○ More Or Less Disagree
- ○ Undecided
- ○ More Or Less Agree
- ○ Agree
- ○ Strongly Agree

Figure A.10.1 Screenshot of items measuring secondary crisis communication

A.11 Manipulation check questions

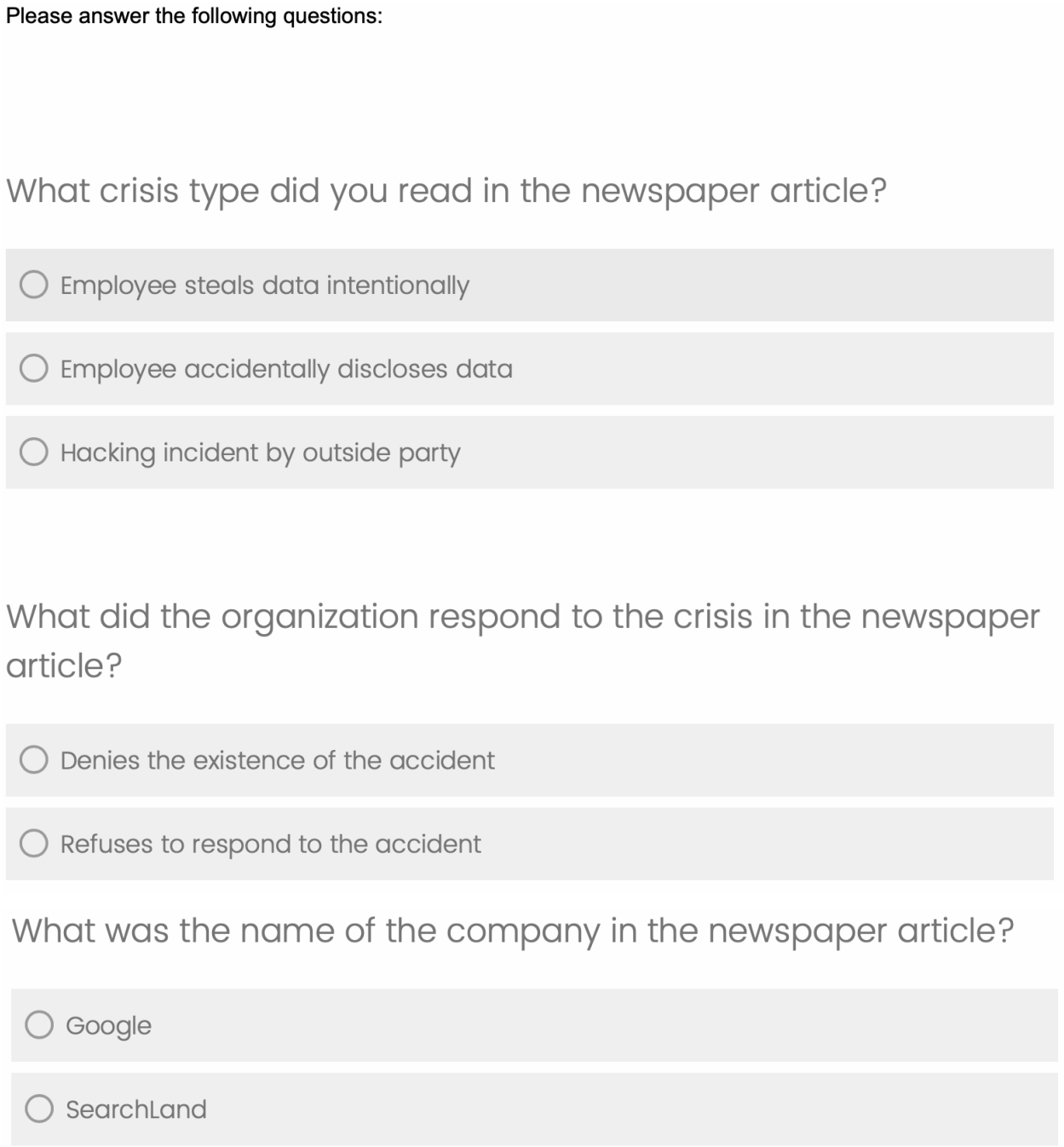


Figure A.11.1 Screenshot of manipulation check questions for data breach crisis type, crisis response strategy and pre-crisis reputation

A.12 Demographic questions

Please answer the following questions:

What is your age?

What is your gender?

- ○ Male
- ○ Female
- ○ Other

What is your nationality?

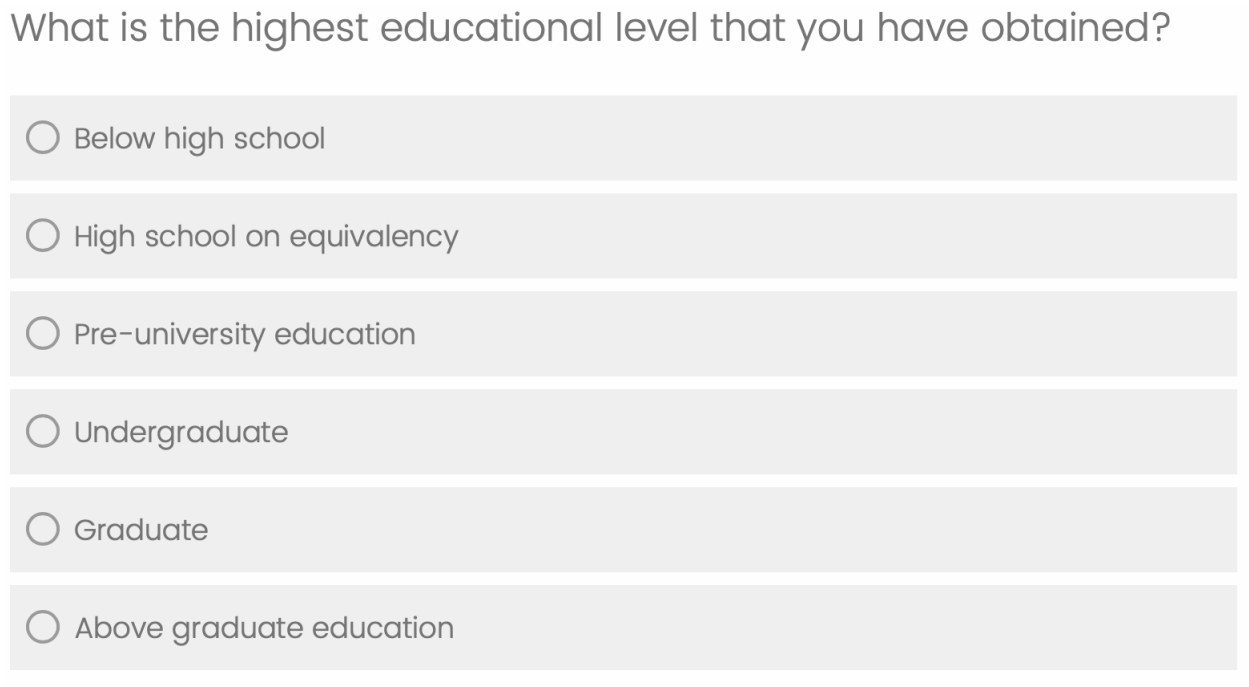


Figure A.12.1 Screenshot op demographic questions

A.13 Debriefing

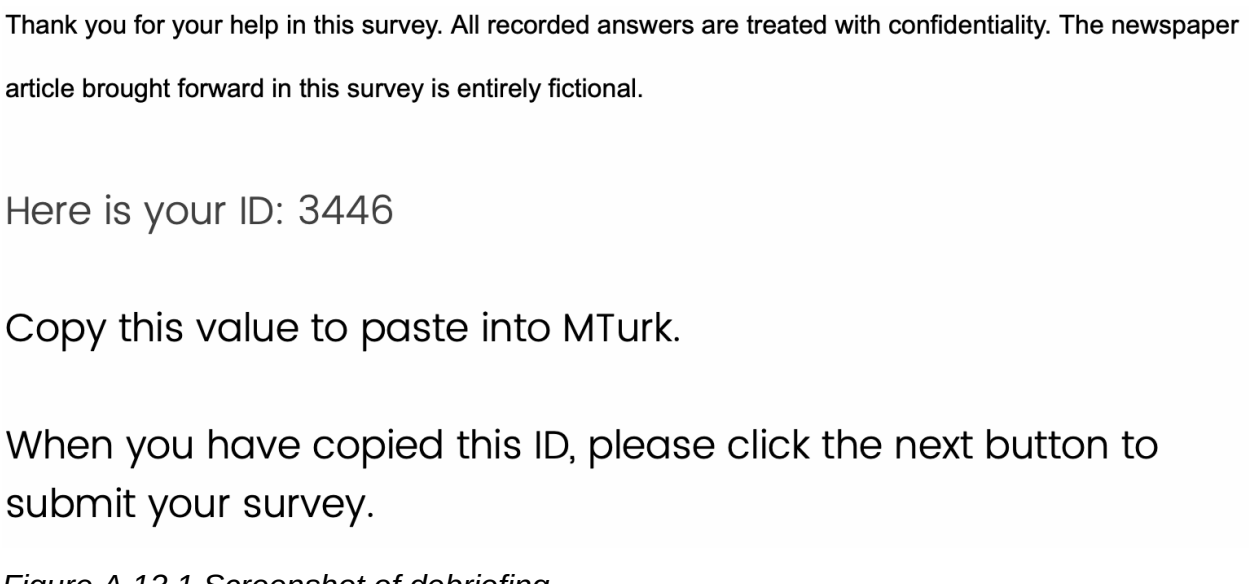


Figure A.13.1 Screenshot of debriefing