UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

THE EFFECTS OF APOLOGIES AND CAUSAL ATTRIBUTION ON PUBLIC RESPONSES

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By
THAM THI NGUYEN
Norman, Oklahoma
2019

THE EFFECTS OF APOLOGIES AND CAUSAL ATTRIBUTION ON PUBLIC RESPONSES

A DISSERTATION APPROVED FOR THE

GAYLORD COLLEGE OF JOURNALISM AND MASS COMMUNICATION

BY

Dr. Doyle Yoon, Chair

Dr. Glenn Leshner

Dr. Sun Kyong (Sunny) Lee

Dr. Jensen Moore

Dr. Jeong-Nam Kim

Acknowledgements

I would like to acknowledge several special people without whom this dissertation would not have been possible. I would like to express the deepest gratitude to my advisor and committee chair Dr. Doyle Yoon, whose profound knowledge and scholarly experience have guided me throughout my doctoral program. I also deeply appreciate his advice and support during the last several weeks, without which this work would not have been a success.

I also appreciate Dr. Glenn Leshner and Dr. Jensen Moore for giving advice that helped me to complete this work. Many thanks to Dr. Sunny Lee and Dr. Jeong-Nam Kim for the encouragement and contributions to this study that helped me to improve it notably. Thanks to my friends, Jocelyn Pedersen and Lucy Mahaffey, who have always been a support to me throughout my graduate studies.

I want to thank my parents, Thai Nguyen and Duong Nguyen, and siblings who have always supported me and encouraged my personal goals. Thanks to my friends in Vietnam and the United States. Special gratitude goes to the participants in the pretest study and the actual study who generously shared their experience, knowledge, and time.

Table of Contents

List of Tables

Abstract

Apologies have been used in crisis communications to address organizational transgressions. Yet, there is no consensus about the components of an apology (e.g., Hearit, 2006; Smith, 2008). Also, the causes of an organization's transgression could affect an individuals' attribution of responsibility toward the organization, which in turn makes a difference to public responses regarding the crisis situation. This study uses data breach crises as examples. Data breaches have become so commonplace that no organization is immune to the dangers of identity theft in the digital world. Organizations whose consumers' personally identifiable information has been compromised could trigger consumers' anger, damage organizational reputation, and injure their trust in the organizations. This study examines the effects of causal attribution and components of apologies, specifically responsibility acceptance and expression of sympathy on public anger relief, organizational reputation, and trust in an organization's competence, integrity, and benevolence. An experimental study used a 2 (causal attribution: internal vs. external) x 3 (explicitness of responsibility acceptance: none, implicit, explicit) x 2 (expression of sympathy: high vs. low) between-subjects design in which participants received sample stimuli in order to measure individuals' judgment on organizational apologies. Findings indicated that there were significant effects of causal attributions on anger relief and trust in an organization's competence and benevolence. Apologies with an explicit statement of responsibility acceptance were found to have significant effects on generating positive perceptions on organizational reputation and regaining trust in the organization's competence, benevolence, and integrity. No significant effects of sympathetic expression were found on dependent variables. There was a marginal interaction effect of causal attribution, responsibility acceptance, and sympathetic expression on public anger relief. No interaction effects between and among the three independent variables were found on other dependent variables. Findings were limited to severe crises because the fictional data breach scenario used in this study revealed a larger number of breached accounts with important personally identifiable information. Discussions about theoretical and practical implications emphasized the role of apology strategy in crisis communications and apologetic components included in an apology statement that could help generate favorable public responses.

Keywords: crisis communications, apologies, responsibility acceptance, sympathetic expression, causal attribution, anger relief, reputation, and trust.

Chapter 1: Introduction

Data breaches can occur at any organization. A *breach* refers to an incident in which personally identifiable information, including individual's name, social security number, driver's license number, medical record, or financial record/credit/debit card are put at risk of identity theft (Identity Theft Resource Center, 2017). According to the Identity Theft Resource Center, in 2017, there were 1,579 reported breaches that were responsible for nearly 179 million exposed records. At the similar reporting date, the Privacy Rights Clearinghouse puts the number of breached records much higher, reporting that more than 1.9 billion records involved in 629 breaches. Data breaches can happen to a wide range of industries. The Identity Theft Resource Center (2017) reported cases in business (55.1%), medical/healthcare (23.7%), banking/credit/financial (8.5%), education (8.0%), and government/military (4.7%). Yet, in many cases, the organizations whose systems were attacked by hackers provided minimum guidance or did not act with speed to notify affected people (Veltsos, 2012).

In 46 out of 50 states in the United States, organizations are required by state laws to notify consumers in the event of a data breach (the law does not apply in Alabama, Kentucky, New Mexico, and South Dakota) (Romanosky, Telang, & Acquisti, 2011). This regulation is important as organizations may hesitate to reveal such negative incidents out of fear of drawing unnecessary attention to the crisis, legal liability, or other related problems (Claeys, 2017). Data breach notification laws differ in many states, but a notification must address five elements: (1) the type of breached personal information (e.g., social security number, driver's license number), (2) the form of data (e.g., unencrypted, computerized, paper), (3) the time to notify individuals (e.g., most expedient time possible, or within 30, 45, or 90 days after discovery of a breach), (4) the form of notice (e.g., newspapers, email, conspicuous posting on the organization's website), and (5) other required content (i.e., organization's contact information). An organization must refer to its state laws to know what must be included in breach notices to affected individuals and state agencies (if any). For example, Massachusetts law recommends organizations to include individuals' rights to obtain a police report, a guidance on requesting a security freeze at no charge, information on complimentary credit monitoring services, and not include the nature of the breach/unauthorized acquisition/use or number of residents affected (201 Code of Massachusetts Regulations 17, 2009). Twenty-five states require organizations to notify data breach incidents to state agencies. Informing the cause(s) of a breach is optional in the notices to individuals, but mandatory to some state agencies (e.g., Virginia). Although organizations must include mandated elements in the notification letter, organizations can control many aspects, such as types of information to be included in the notification letter as required by state laws) through the use of apologies to mitigate reputational damage and rebuild consumer trust.

To date, scholars defined and operationalized organizational apologies inconsistently in crisis communications and thus found inconsistent effects of apologies on public responses (e.g., Bentley, 2014; Coombs & Holladay, 2008; Pace et al., 2010). *Crisis* refers to an event that threatens important stakeholders' expectation to an organization and can impact the organization's performance (Coombs, 2010). The cause(s) of a crisis situation often affects how individuals attribute crisis responsibility to an organization (Coombs & Holladay, 2012). *Causal attribution* refers to the way an individual makes judgments about the self or another person based on their understanding and explanation about the cause(s) of their own or other people's behavior (Weiner, 1975). In this study, causal attribution refers to an individual's judgment on the cause(s) of an organization's transgression or crisis incident. Understanding the cause(s) of a crisis could help individuals to determine whether the crisis is caused by internal/controllable or external/uncontrollable factor(s).

Additionally, an apology could be made for an organization's wrongful actions or the negative effects that the act may have caused (Frandsen & Johansen, 2010). Since there is no consensus on components of an apology, this study focuses on examine two components: responsibility acceptance that was identified as the most important component in organizational apologies ((Lewicki et al., 2016) and sympathetic expression which was recommended to use for relieving public anger. *Responsibility acceptance* refers to the extent to which an organization claims their accountability, or having a duty to deal with, something, specifically a crisis (Pace et al., 2012). *Expression of sympathy* refers to the extent with which one expresses his or her concerns and how whatever affected the other would have an impact on his or herself (Chung & Lee, 2012). In crisis communications, an organization may choose to express sympathy at low or high level toward the affected individuals. This study examines the effects of apologies in crisis communications, specifically the relationships between (1) responsibility acceptance and expression of sympathy in an apology, and (2) causal attribution to a crisis situation as independent variables, and (3) public responses, such as public anger relief, organizational reputation, and trust antecedents, including competence, integrity, and benevolence. Potential implications include identifying apologetic components used in different causal attributed conditions in transgression-based crises that could help to reduce public's anger, mitigate reputational damage, and rebuild individuals' trust in the organization.

Apology

Apologies were found to be effective in addressing interpersonal offenses and certain crisis situations (e.g., Benoit & Brew, 1997; Coombs & Holladay, 2008; Lyon & Cameron;

2004). Although Benoit (1995) contended that making an apology means admitting guilt and seeking forgiveness, Hearit (2006) argued that an apology does not always mean accepting responsibility, instead it can be viewed as a social ritual that offenders use to express remorse for their actions and their desire to follow social norms in the future. Depending on the cause(s) of a crisis situation and the components included in an organization's apology, individuals can interpret the apologetic messages and react to the organization's crisis responses differently. Yet, the question is what components of an apology should be included to contribute the most in gaining favorable public responses.

Although scholars in different fields hold different opinions about what components constitute an apology (Coombs et al., 2010; Benoit, 2015), several common components were recommended to maximize the effectiveness of apologies in interpersonal relationships (e.g., Lazare, 2004; Scher & Danley, 1997; Tavuchi, 1991). An apology should acknowledge the offense, express regret, and promise not to repeat the offense (e.g., It won't happen again) (Lazare, 2004, Tavuchis, 1991). To maximize the psychological effectiveness of apologies, Lazare (2004) also recommended offering reparation for the harm caused by the offense. In a psychology study, Scher and Danley (1997) identified four elements of apology-functioning speech act, including acknowledging responsibility, expressing regret, promising of forbearance, and offering reparations. These four elements were found to be useful in Bisel and Messersmith's organizational communication study (2012). Studies in crisis communication found responsibility acceptance the most important component in organizational apologies (Lewicki et al., 2016), while sympathetic expression was suggested as an alternative option when crisis responsibility is perceived to be mild (Bennett & Earwalker, 2001). Thus, this study focuses on examining the effects of accepting responsibility and sympathetic expression.

Making an apology could be a risky choice as it could create legal concerns. Although existing studies found the effects of organizational apology in protecting reputations, accepting responsibility in an apology could be used against the organization in legal courts (Patel & Reinsch, 2003). However, state laws sometimes do not consider apologies as evidence at trial (Myers, 2016). Robbennolt (2006) argued that sympathetic statements could reduce the number of lawsuits since plaintiffs sometimes seek an apology rather than monetary reward at a court. Thus, sympathetic expression can sometimes be used instead of accepting responsibility in an apology (Coombs & Holladay, 2012). Yet, the question in what situations the organization should use sympathetic expression and how sympathetic expression affects public responses.

Apologetic responses were more effective than defensive responses at creating positive customer impressions toward an organization and motivating them to do business transactions with the organization (Lyon & Cameron, 2004). Stakeholders' interpretation of apologies and how they attribute crisis responsibility can affect the effectiveness of an apology. Apologies were found to be no more effective at improving attitudes toward an organization than offering compensation or expressing sympathy (Coombs & Holladay, 2008). Coombs and Holladay (2008) treated offering compensation as a separate crisis response, while other studies (i.e., Bentley, 2014; Bentley et al., 2018) considered compensation as a part of corrective actions embedded in an apology statement. Accepting responsibility and expressing remorse appear to be more effective in organizational apologies that contribute to reduce public anger and mitigate reputation damage (Pace, Fediuk, & Botero, 2010). Yet, findings in Pace et al.'s study did not consider how causal attribution could affect the effects of accepting responsibility and remorse expression. Thus, this study examined the effects of causal attribution, as one of independent variables, on public responses.

At different levels of crisis responsibility, the effects of sympathetic expression and responsibility acceptance could vary. Chung and Lee (2017) noted that a responsibility-oriented apology was more likely to reduce public anger, negative impression, and distrust to a company than a sympathetic-oriented apology in an internal/controllable crisis situation. There were no interaction effects between responsibility admittance (active vs. passive) and sympathetic expression (high vs. low) on public anger relief (Chung & Lee, 2017). This study argues that an organization could choose to explicitly or implicitly accept responsibility to avoid creating disadvantaged evidence in legal courts. In other words, the explicitness of responsibility acceptance could yield different effects. Moreover, public trust or distrust in organization could vary at different aspects of the organization's competence, integrity, and benevolence. Although explicitly accepting responsibility could reduce public anger (e.g., Chung & Lee, 2017; Pace et al., 2012), an apology that include both components of responsibility acceptance and sympathetic expression could yield better public responses than an apology having either one of these two components.

Developing effective crisis communication responses requires an understanding of customer trust. Trust is one of the key elements in establishing and maintaining organization-consumer relationship (Liu & Mehta, 2017; Kang & Hustvedt, 2014). Once the customers perceived they are treated fairly, they tend to return repeatedly when in need of a good or service from the organization. On average, high-trust organizations outperformed low-trust organizations by 286 percent of return to shareholders (Cover, 2006). In contrast, losing customers' trust could cause financial damage and other consequences. The E.coli breakout in October 2015 cost Chipotle significantly in terms of losing revenue, market share, and expenses for launching a marketing communication campaign to win back customers' trust out of food-safety fear (Jargon, 2016).

In data breach situations, customers entrust the organization with their information, thus if anything goes wrong, the organization needs to be transparent and act quickly to protect effected customers. Although trust has been examined in various disciplines, such as sociology, psychology, management, philosophy, organization communication, and media studies, research gaps regarding trust in crisis communications exist. Specifically, several research topics fall short on examining trust in risk and crisis communications, including an agreement on a definition to guide appropriate trust measurements, comprehensive trust theory, insights on how crisis communication messages influence trust, the role of trust in risk and crisis communications, trust over time and across crisis management stages (Liu & Mehta, 2017). In addition to understanding the effect of different apologetic components and causal attribution on anger relief, perceived organizational reputation, this study also aimed to understand how an apology could help to rebuild trust in the organization in the wake of a crisis, specifically data breach crises.

Background of Data Breach Crises

This study examined crisis communications using a fictional data breach scenario as this is a new crisis type in the digital age, and both organizations and their affected customers are viewed as victims in the incident (Bentley, 2018, Veltsos, 2012). Data breaches encompass issues in cybersecurity and the potential risks of leaking personally identifiable information. Personally identifiable information is gathered by database centers that hold lots of sensitive information in one place and can be used to distinguish or trace an individual's identity. A data breach may occur intentionally or unintentionally in either electronic or paper format. Based on the causal attribution concept discussed in the Situational Crisis Communication Theory (SCCT), the intentional or unintentional causes of a data breach affects individuals' interpretation on whether the incident was caused by internal or external factors and whether the organization could control the situation. Thereby, it affects individuals' attribution on crisis responsibility toward the organization.

Common reasons of data breach crises are loss of equipment, unintentional leaks, illegal sales of personal information, or outright data theft (Friedman & Telang, 2006). Identity theft may occur through hacking data centers at organizations or conducting data mining to find similarities and put together an accurate profile from pieces of personal information when people sign up for using services, social networking sites, or when they register software after making purchases (Friedman & Telang, 2006). Some people may not have sufficient knowledge of how identity theft works, some may feel safe with providing bits of personal information which are not stored in one place. Yet, once identity thieves find the right combination of data, consequences never end for victims because personally identifiable information does not change. Once personally identifiable information is stolen, identity thieves will use it many times to spend money from the victim's bank account or apply for mortgages or credit cards (Rode, 2007).

Data breach notification. Data breach notification state laws require organizations to notify affected stakeholders to avoid optimism bias (i.e., "It can't happen to me") and overcome rational ignorance (i.e., "It's not worth the time and trouble") (Romanosky, Telang, & Acquisti, 2011; Veltsos, 2012). Data breach notifications inform affected people about the breach so they can act on protecting themselves as well as encouraging organizations to improve their information security system (Romanosky et al., 2011). This study uses the two terms *notification* *letter of a data breach (or notification letter)* and *notice of a data breach* interchangeably. The *notification letter* refers to the letter that an organization sends via email or mailing to its impacted customers*,* while the *notice of a data breach* (also known as *open letter*) is published on the organization's website, a designated blog, and could be covered by the media. The content of the notification or notice of a data breach is almost the same. The notification letter may have a few differences in formatting, such as including a salutation (e.g., Dear [organization name] guests/customers) and being signed by a leader of the organization or cybersecurity or equivalent department/division (Jenkins, Anandarajan, & D'Ovidio, 2014).

Crisis communication messages are embedded in the notification letter (Bentley, 2014; Veltsos, 2012). The notification letter must aim to convince readers about the existence of a potential risk and encourage them to act on preventing potential harm that might arise from a data breach event. A data breach can be a public relations nightmare that threatens an organization's reputation and credibility (Veltsos, 2012). Crisis communications must provide data breach notifications that comply with notification laws and repair organizational image, rebuild customers' trust, and mitigate civil liability (Bentley, Oostman, & Shah, 2018; Jenkins et al., 2014). Since a data breach incident is bad news, crisis communications should provide notifications to protect customers and reinforce customers' trust in organizations. Along with providing information as required by law, an apology strategy is recommended to use in notification letters when a data breach occurs (Jenskins et al., 2014).

A notification letter should address the breach with adequate amounts and types of information outlining what was stolen by hackers and guide consumers through the process of dealing with the data breach news (Jenkins et al., 2014). Failing to address the breach may influence consumers' decisions about continuing or ceasing a relation with the organization.

Although a notification letter is mandated by law, consumers receiving this letter without any prior warning may feel distrust and temper their anger toward the breached company. Thus, the letter's content should reflect good strategic sense to mitigate the consumers' negative experience.

A typical notification letter contains a description or summary of what happened, the type of information that was lost, the date of the occurrence, what the organization is doing to fix the issue (if any), what consumers can do, and contact information for more information or identity theft prevention tips. Thus, organizations should include *explanations* and employ *politeness* strategies when expressing bad news in the notification letter. *Explanation* includes the description and summary of the data breach (Jenkins et al., 2014). Explaining the negative information to the receivers does not only reflect a moral obligation of a responsive organization, but also does not cause people to feel disregarded or feel like they are being deceived. *Politeness* in a notification letter includes an apology and expresses the breached company's willingness to pay for a third-party identity theft protection service (Jenkins et al., 2014) or other corrective actions to protect the company's database from continuing to be hacked. Providing explanations is also viewed as a politeness strategy itself in protecting the organizational image (Brown & Levinson, 1987; Campbell, 1990).

Some studies treated a notification letter as an apology (if the organization chose to apologize) (e.g., Bentley, 2014; Bentley et al., 2018), while others viewed the apology as a strategy being used along with other crisis communication strategies embedded in the notification letter (e.g., Jenkins et al., 2014; Kim, Johnson, & Park, 2017). Bentley et al. (2018) argued that apologies in crisis communications should include words (e.g., express genuine remorse, acknowledge their worth, affirm their values, emphasize with their suffering, and request another chance) and actions (e.g., provide compensation or foster personal communication) to fix the problem and rebuild stakeholders' trust in data breaches. In Bentley et al.'s study (2018), crises were categorized into two types: (1) ambiguous responsibility crisis situations including only data breaches and (2) clear responsibility or direct blame for any other crisis cases. Bentley et al. (2018) argued that data breach crises are unique in that consumers may perceive the hacked organization as the victim since no organization would want their customer database to be hacked. On the other hand, consumers may attribute high crisis responsibility to organizations because they think the company breached consumer trust and their commitment to protecting private data. Yet, the classification of crisis responsibility as clear and ambiguous in Bentley et al.' (2018) study was debatable. According to SCCT, customers can attribute crisis responsibility in situations when the causes of the data breach can be identified. Being able to identify the cause can, in turn, help to determine if the organization's actions were unintentional or intentional.

It is true that affected customers or key stakeholders could attribute certain level of crisis responsibility to the organization regardless the cause(s) of the incident because the organization failed to protect their customers' information. Understanding the cause(s) of a data breach incident (e.g., management's failure within an organization or skilled black hackers) does not set the organization free from crisis responsibility. Instead, the cause(s) of a data breach incident enables individuals to determine who is primarily responsible for the crisis. SCCT emphasized the ways crisis response strategies and crisis responsibility impact organization's reputation. Thus, this study aimed to identify elements of an apology, viewing it as a strategy used along with other crisis communication strategies embedded in a notification letter. In this case, crisis responsibility can be determined based on the cause of a data breach crisis that helps to determine the threat to an organization’s reputation and crisis responsibility attribution.

Problem Statement

This study questions the effect of each variable, specially, causal attribution, responsibility acceptance, and sympathetic expression on public responses. The study also aims to understand the extent to which the explicitness of responsibility acceptance and the level of sympathetic expression, at different causal attributed conditions, could affect public responses. Can an apology including responsibility acceptance and sympathetic expression generate more favorable public responses compared with an apology including either one of these two different components? What is the interaction effect of sympathetic expression and responsibility acceptance on public’s responses at different causal attributed conditions? In the context of a trust violation scenario, an apology could be used in an effort to repair trust. The next question is whether accepting responsibility is more effective in regaining public trust in an organization’s competence, integrity, and benevolence than a sympathetic expression? Thus, this study seeks to identify which levels of explicitness in responsibility acceptance and sympathetic expression at different causal attributed conditions can generate favorable public responses.

The Purpose of the Study

The purpose of this study is to examine the effects of apologetic components, specifically responsibility acceptance and sympathetic expression, and causal attribution on public responses, including, public anger relief, organizational reputation, and trust in the organization’s competence, integrity, and benevolence. A fictional data breach crisis in an experimental design setting is used to test these relationships. The study argues that whether the situation is controllable or not and caused by internal or external factors, both the organization and their customers are victims in the incident (Bentley et al., 2018). Thus, it could affect stakeholders' determination on who is primarily responsible for a data breach crisis.

The study focuses on two issues. First, the study examines how accepting responsibility for a transgression, sympathetic expression, and causal attribution could affect public responses. Second, the study investigates the interaction effects of causal attribution, responsibility acceptance, and sympathetic expression on public responses. Understanding the effects of causal attribution and apologetic components can improve the ways organizations communicate when a transgression occurs, thereby contributing to an organizations' efforts to gain favorable public responses.

This study is based on two assumptions. The first assumption is that organizational reputation is threatened by crises. This assumption is mentioned in the Situational Crisis Communication Theory, which acknowledges the need to address public safety, before addressing reputational concerns (Coombs, 1999; Coombs & Holladay, 2001, 2002). The second assumption is that trust in an organization is reduced or lost when a crisis occurs, as the organization failed to fulfill their commitments or does not meet public's expectation (Coombs, 2010). Thus, it is important to use an apology appropriately in the attempt to rebuild public trust.

Theoretical Framework

This study reviewed literature from three research areas, primarily crisis communications, organizational reputation, and trust. The first field of research was crisis communications. Crisis management and communications aim to prevent harms to others and be accountable for actions during the crisis (Coombs & Holladay, 2001). Thereby, crisis managers become legitimate participants in a community or groups of affected stakeholders. Some researchers consider a crisis to be a mistake, managerial failure, or even violation of laws or ethics (e.g., Lewicki et al, 2016), while other scholars focus on the inadequate control needed to prevent, mitigate, respond, and learn from a crisis (e.g., Coombs, 1999). Some researchers view a crisis as risk manifested—a risk management failure that has turned into a crisis (e.g., accounting fraud causing financial crisis, failing to ensure safety standards leading to product recalls) (Reynolds & Seeger, 2005). This study employs two theories in crisis communications, Image Restoration Theory (IRT) and Situational Crisis Communication Theory (SCCT), to examine the effects of apology strategies in crisis communications in protecting organizational reputation and rebuilding public trust in the organization.

Image Restoration Theory (IRT) posits that organizations should act to protect their public image or reputation when key stakeholders' perceived their acts are offensive (Benoit, 1995, 1997, 2015). Perception is fundamental to image restoration since it motivates the accused actor to take a defensive strategy when the actor is perceived to hold responsible for an action. IRT was developed based on the assumption that maintaining a favorable reputation is a key goal of communication that could be achieved through directed activities. Benoit and Pang (2008) argued that apologizing is the most appropriate strategy when organizations are at fault. However, due to the concerns of possibly creating evidence of guilt in litigation, apologies were suggested to be the last option in crisis communications (Hearit, 2006). Also, Benoit (2015) claims that IRT focuses on identifying options rather than prescribing solutions. Therefore, choosing appropriate crisis response strategies in different situations is crucial, and SCCT aims to address this issue.

Situational Crisis Communication Theory (SCCT) is a crisis communications theory developed by Timothy Coombs and colleagues. SCCT posits that organizational reputation is threatened in the wake of a crisis (Coombs, 1995; Coombs & Holladay, 1996). Thus, crisis managers should match crisis response strategies to the level of crisis responsibility and reputational threat posed by a crisis (Coombs & Holladay, 1996). SCCT roots in attribution theory suggesting that individuals tend to find causes, or make attributions, for events, especially when the events are negative or unexpected. SCCT focuses on identifying and evaluating key facets of a crisis situation, such as crisis type, crisis history, and prior relationship reputation, to predict organization's reputational threat as well as public's perception of the crisis and their attribution on crisis responsibility (Coombs, 2007). Evidence-based assessment allows crisis managers to make informed, strategic crisis responses.

The second field of study was organizational reputation. The term *reputation* has been studied for more than three decades with different conceptualizations. Barneet et al. (2006) defined reputation as a state of awareness, an assessment, and an asset. As a state of awareness, reputation reflects stakeholders' general perception of an organization without making a judgment about it. Assessment includes a judgment of corporate reputation. Corporate reputation is also viewed as an intangible, financial or economic asset. Thus, corporate reputation reflects 'observers' collective judgments of a corporation, based on assessments of the financial, social, and environmental impacts attributed to the corporation over time" (Barneet et al., 2006, p. 9). Corporate reputation encompasses four constructs, including (1) corporate identity – collection of symbols, (2) corporate image – impressions of the firms, (3) corporate reputation – observers' judgments, and (4) corporate reputational capital – economic assets (Barneet et al., 2006). This study focused on examining the corporate reputation construct. Since reputation can be found at any types of organization, this study used the term *organizational reputation* instead of corporate reputation. Judgment of organizational reputation can be formed from individuals' perceptions of the organizational identity and impressions of its image, but often occurs as a consequence of a trigger event, such as a crisis incident (Barneet et al., 2006). Thus, reputation is fundamental for organization’s success in handling crisis situations, specifically, when organizations use apologies as crisis responses.

The third field of study was trust. From the interpersonal trust perspective, trust refers to the expectation that another party will perform a particular action (Mayer, Davis, & Schoorman, 1995; Rousseau et al., 1998), or the intention to accept vulnerability to a trustee, based on positive expectations of an individual or organization’s actions (Colquitt et al., 2007). Trust is formulated based on a cognitive process of evaluating different factors that help an individual decides if a person or organization is trustworthy, untrustworthy, or unknown (Lewis & Weigert, 1985). Thus, *trustworthiness,* including three antecedents such as competence, integrity, and benevolence, is central in understanding and predicting trust levels (Colquitt et al., 2007). In this study, trust, as a dependent variable, was measured in terms of an organization’s competence, integrity, and benevolence. *Trust in competence* refers to knowledge, skills, and characteristics in some specific area that trustee or employees of an organization have that could earn people trust on them in performing tasks related to that area (Mayer et al, 1995; Zand, 1972). *Trust in benevolence* refers to the positive perception of trustee toward the trustor (Mayer et al., 1995). In this study, it refers to stakeholders (trustee) trust that can develop through emotional bonds with the organization, that in turn enhance affective bonds and interaction with the organization (Williams, 2001). *Trust in integrity* is evaluated based on the consistency between the organization’s values and its behavior, and the organization adheres to principles of fairness (Mayer et al., 1995).

Summary

This chapter introduced the background of the study and data breach crises, problem statement, purpose of the study, theoretical framework, and outlined definitions of key terms. The following sections included four chapters, references, and appendices. Chapter two reviewed literature of relevant crisis communications theories and existing studies in apology strategy, anger relief, reputation, and trust. Chapter three outlined the methodology of the study, study population and sampling, stimuli, the procedures of the pretest and main study. Chapter four reported findings. Chapter five discussed the findings, theoretical and practical implications, strengths and limitations, suggestions for future research, and conclusions.

Chapter 2: Literature Review

Image Restoration Theory

How scholars conceptualize a crisis determines the interconnection of crisis management with issues, brand equity, and risk management or even the assessment on the effectiveness of various crisis responses. Although communication is essential in all crisis management phases, researchers have tended to focus on the crisis response phase that seeks to respond to crises appropriately and in a timely manner (Coombs, 2010). Two prominent theories that seek to identify the right crisis response strategies to protect and rebuild an organization's reputation include (William) Benoit's Image Restoration Theory and Situational Crisis Communication Theory (SCCT) posited by W. Timothy Coombs.

Image restoration theory (IRT), introduced by William Benoit, was developed based on theories of apologia and accounts. Apologia refers to a formal defense that an individual or organization uses to justify a stance, opinion, and actions (Ware & Linkgel, 1973). An individual or organization makes a statement (also called 'account') to explain an unanticipated event or transgression (Schonbach, 1980; Scott & Lyman, 1968). IRT suggests organizations to use image restoration activities when key stakeholders or public blame them for a transgression. The organization that committed the wrongful act should choose appropriate communication strategies based on situational factors with a consideration of various factors such as stakeholder perceptions about the transgression, degree of the act's offensiveness, and organizational credibility (Benoit, 1995). The goal of communication is to maintain an organization's favorable reputation (Benoit, 1995).

Benoit (1995) identified five broad categories of image restoration strategies that could be used to respond to different threats, including denial, evasion of responsibility, reducing offensiveness, corrective action, and mortification. Denial and evasion of responsibility strategies could be used when the organization chooses to take a defensive stance by rejecting or attempting to reduce the level of crisis responsibility. Denial has two approaches, including shifting the blame to another person or organization outside the boundaries of the organization, or denying false charge or responsibility of an action (e.g., Benoit & Czerwinski, 1997; Benoit & Hanczor, 1994. Evasion of responsibility can be made three ways: by claiming the action is a reasonable reaction to an incident; by defeasibility (i.e., an excuse of lacking of information or control over something); or claiming an action occurred by accident or was primarily performed with good intentions (e.g., Brinson & Benoit, 1996).

Reducing offensiveness and corrective action strategies are recommended when an organization attempts to reduce the offensiveness of the act attributed to the accused or the organization (Benoit, 1995). Reducing offensiveness can be performed in six ways, including (1) bolstering strategy by strengthening stakeholders' positive feelings toward the organization, (2) minimizing negative feelings related to the wrongful act, (3) differentiation by referring to other similar but more offensive actions committed by other organizations, (4) transcendence by placing the act in a more favorable context, (5) attack the accusers, and (6) compensation. Corrective action strategy includes a promise embedded in a crisis communication message that shows the organization's efforts to correct the problem. The final strategy for image restoration is mortification which suggests that the accused should not only admit culpability but also ask for forgiveness (i.e., apology) (e.g, Brinson & Benoit, 1994, 1999).

Using a mortification strategy or an apology is considered to be a last option since it has potential drawbacks including the possibility of lawsuits (Hearit, 2006). However, apologizing for an action or transgression indicates ethical crisis responses and could maintain the organizational credibility (Benoit & Pang, 2008). Moreover, apologizing does not always create evidence or leave the organization in question at a disadvantages in lawsuits (Patel & Reinsch, 2003). Thus, apologies are necessary for organizations that seek to protect their reputation or public image (Benoit, 1995, 1997). Since IRT primarily focuses on identifying crisis response options, this study also uses SCCT that aims to suggest solutions to address a crisis.

Situational Crisis Communication Theory

SCCT provides a framework for crisis communication scholars and practitioners to understand and choose appropriate crisis response strategies that aim to protect an organization's reputation. This study used SCCT to make arguments for protecting organizational reputation and repairing stakeholders' trust in an organization in the wake of a crisis. Situational Crisis Communication Theory (SCCT) is rooted in attribution theory (Weiner, 1986) which argues that people observe and attribute other individuals or organizations' actions in consideration of three factors of causal attribution: stability versus instability, controllability versus uncontrollability, and internality versus externality. *Stability* means whether causes of an incident or event change over time. *Locus of control* focuses on determining whether internal or external factor(s) causes the incident. *Controllability* questions whether an individual or organization involved in the incident can control the causes (e.g., skills) or cannot control it due to other factors (e.g., out of luck) (Weiner, 1986). This study examined causal attribution based on locus of control and controllability, and did not focus on the changes over time of the cause(s).

People tend to attribute stronger attributions of responsibility when they believe the actor was in control of the action or when the act was representative of the actor’s true character (Coombs & Holladay, 2002). While stronger attributions of responsibility can trigger anger, people tend to be sympathetic to the actor when they attribute weaker responsibility to the actor’s transgression (Weiner, 2006). Based on the argument for individuals’ judgment of crisis responsibility and the level of reputational threat, Coombs (2007) categorized crises into three clusters in organizational crises (Coombs, 2007). The victim cluster, including disasters, rumor, product tampering, and workplace violence, yields weak responsibility attribution to an organization as the organization is also a victim of the crisis, along with its stakeholders. The accidental cluster produces moderate responsibility attribution to the organization although the act was unintentional, but a result of organizational mistakes (e.g., product recall, industrial accidents). Finally, the preventable cluster produces the strongest attribution of responsibility as the crises occurred as a result of organizational misconduct (e.g., laws/regulations violation, extreme negligence that places people at risk). Depending on the cause(s) and severity of a data breach crisis, it could be classified into victim cluster (e.g., hacker(s) found (a) week point(s) in an organization’s firewall and get access to its database), accidental cluster (e.g., an unintentional accident occured and an orgaziation’s database were hacked), or preventable cluster (e.g., an employee’s mistake causing information leaked from the system).

SCCT suggests that strategic crisis responses should be chosen in consideration of the level of crisis responsibility and reputational threat posed by a crisis (Coombs, 1995). Although Coombs (1995) did not mention apology in the crisis communication matrix, the matrix’s mortification strategy including remediation, repentance, and rectification contain a level of fault admission or apology. An apology is expected when the organization fails to meet stakeholders’ expectation and/or when public anger is high (Coombs, 2013). Yet, an apology was not always the best practice in crisis communications since an expression of sympathy or compassion could yield the same effect in certain circumstance (Coombs & Holladay, 2008).

Coombs (2007) categorized crisis response strategies into two major groups that are named as the primary and secondary crisis response strategies. The primary crisis response strategies listed three sub-groups that seeking to deny, diminish, or rebuild. Deny strategies, including attack the accuser, denial or scapegoat, aim to shift blame or claim no crisis that are appropriate to respond to crises in the victim cluster. Diminish strategies seek to excuse or justify the situations that tend to work in accidental crises. Rebuild strategies, including compensation and apology strategies, are the most appropriate ones in preventable crises. Since data breach crises could affect negatively to public responses, this study focused on rebuild strategies that aim to maintain and rebuild public-organization relationships.

Understanding how stakeholders attribute crisis responsibility to an organization helps crisis managers to select appropriate crisis response strategies. Thereby, it could affect organization-public relationships in which trust between two parties is an important factor. Individuals' anger toward the organization could lead to negative word-of-mouth or even cease relationships with the organization (Choi & Lin, 2009; Coombs & Holladay, 2008). Thus, an organization may choose to use an apology in its crisis responses. According to SCCT, an apology should indicate that the organization takes full crisis responsibility and asks for stakeholders' forgiveness (Coombs, 2007). Yet, existing studies contended that organizational apologies do not always claim full responsibility acceptance (e.g., Chung, 2006; Pace et al., 2010; Lewicki et al, 2016).

Individuals make judgment based on causal attribution to a crisis in order to blame or attribute crisis responsibility toward a specific organization or individuals (Coombs, 2007). Using experimental studies to examine the effects of various crisis communication strategies, Coombs and colleagues suggested that crisis managers seek to select appropriate crisis response strategies to protect victim(s) (if any) and mitigate corporate reputational damage (e.g., Coombs, 1995; Coombs & Holladay, 1996). Apology strategies in crisis responses could aim to take the critics' focus away from the crisis in consideration of crisis responsibility attribution and reputational threats to the organization.

Apology in Crisis Communications

An apology could be made for an organization's wrongful actions or the negative effects that the act may have caused (Grandson & Johansen, 2010). Failing to apologize appropriately can damage organization-public relationships, organization's reputations and miss the opportunities to rebuild public's trust in the organization (Schweitzer, Brooks, & Galinsky, 2015). There are various considerations on who, what, when, where, and how to apologize appropriately. This study focuses on what to say in apologies. Schweitzer et al. (2015) suggested that an effective apology should achieve three goals: be candid (the organization acknowledges the harms caused by the crisis and its own responsibility), express remorse for transgression(s), and promise to change in order to prevent similar transgressions from happening again. The organizational apology can post a dilemma in saying apologies or not. Apologies were considered as risky and uncomfortable, making some organizations seek reasons to delay or using apology strategies. An organization can take defensive stance, shift blame to others, or avoid taking responsibility when evaluating the situation through a legal lens (Schweitzer et al., 2015). The liability constrain can motivate organization executives or crisis managers to use strategic ambiguity or equivocal communication (Eisenberg, 1984). Equivocal communication refers to a strategy in which the message appears to be non-straightforward, ambiguous, obscure, or even evasive about the organization's responsibility to the incident (Bavelas, Black, Chovil, & Mullett, 1990). Using strategic ambiguity to avoid bearing some responsibility may leave stakeholders dissatisfied, humiliated, anger, and demand an apology (Tyler, 1997). Also, discouraging apologies due to concerns about liability constrain could lead stakeholders to react defensively and worsen the situation.

An apology used as a crisis response strategy should adhere to ethical standards, including being truthful, sincere, voluntary, timely, addressing all stakeholders and be performed in an appropriate context (Hearit, 2006). A truthful apology suggests not leaving out important information that affects the way people see the wrongful action (Hearit, 2006). A sincere apology must demonstrate the real effort to achieve reconciliation, instead of only trying to address journalists to avoid negative media coverage (Frandsen & Johansen, 2010). The sincerity should be demonstrated at the operational level (e.g., product recall) and at the communicative level (e.g., send an email to inform affected individuals about actions being conducted by the organization) when addressing customers' concerns (Frandsen & Johansen, 2010). In trust violation situations, apologies were more effective when they were perceived to be sincere, and delivered soon after the trust violation (Lewicki, Polin, & Lount, 2016). Since organizations fail to fulfill stakeholders' trust in protecting their personally identifiable information, data breach crises could be considered as trust-based violations. Thus, stakeholders may expect genuine apologies. Additionally, the timeliness of an apology should be considered to avoid any misunderstanding, doubts of condescending any self-interest. An appropriate apology should also address all relevant stakeholders who have been offended or suffered from the wrongdoing in consideration of the context (Frandsen & Johansen, 2010). Moreover, existing crisis communication studies considered responsibility acceptance the most important component in organizational apologies (e.g., Lewicki et al., 2016), while sympathetic expression was recommended when crisis responsibility is perceived to be mild (Bennett & Earwalker, 2001).

Accepting responsibility, also called as *acknowledgment of responsibility,* is defined as "a statement which demonstrates the violator understands their part in the offence" (Lewicki, Polin, & Lount, 2016, p. 178). This definition indicates that the acknowledgment of responsibility should be claimed explicitly. For example, "I was wrong in what I did, and I accepted responsibility for my actions" (Lewicki et al., 2016, p. 178). Yet, not all apologies explicitly accept responsibility, instead, an apology may simply inform the occurrence of the crisis or implicitly accept responsibility.

Wispe (1986) defined sympathy as "the heightened awareness of the suffering of another person as something to be alleviated" (p. 318). This notion considered two aspects: (1) the increased sensitivity to other person' emotions and (2) the urge to take mitigating actions to alleviate the suffering that the other person is experienced (Mercer, 1972; Wispe, 1986). There is a subtle distinction between sympathy and empathy. While sympathy is a way for the sympathizer to "relate" or "move by" the other person, empathy is a way for the empathizer to "know" or "reach out" for the other person (Barrett-Lennard, 1962; Wispe, 1986). A sympathetic expression not only intensifies the emotional sensitivity of people suffering from a predicament, but also expresses a compassion feeling and the urge to help those people (Wispe, 1986). Wispe (1986) questions three important aspects of a sympathetic expression, including (1) how a person expresses sympathy, (2) how the sufferer knows when the person is sympathizing, and (3) what the sympathizer really feels for their own sympathetic expression. This study focused on understanding individuals' feelings of anger after reading a statement of sympathy that is manipulated at either high or low level of sympathy.

Functions of an apology. An apology could serve two general functions, including: (1) fulfilling "social requirement" of acknowledging responsibility when any sort of wrongdoing is done and (2) accompanying emotional expressions to shows additional meaning about the apologist's intentions (Scher & Darley, 1997). First, the *acknowledgement of responsibility* demonstrates the apologist's awareness of the social norm in recognizing the wrongful act (Lewicki, Polin, & Lount, 2016) or reflecting the organization's ethical domain (Ho, 2005). Coombs and Holladay (2008) suggests that accepting responsibility is the "centerpiece of an apology" (p. 253). Victims were found to perceive more positive toward violators that took greater responsibility for wrongful acts (Hoggins & Liebeskind, 2003). Apologies that show responsible acceptance can reduce public anger arising from a crisis situation (Scher & Darley, 1997) and mitigate reputation damage for an organization (Pace, Fediuk, & Botero, 2010). An apology does not only reduce public anger, but also could increase positive emotions (Frantz & Bennigson, 2005; Ohbuchi et al., 1989). Yet, failing to deliver appropriate apology could trigger public anger that motivates them to file a lawsuit (Rosenbaum, 2004). An apology is less likely to be used when attributed responsibility or the severity of the mistake is perceived as mild (Bennett & Earwalker, 2001).

Second, apologies accompanied by emotional expression show the violator's negative feelings for making their wrongful acts (Lewicki, Polin, & Lount, 2016). Expressing regret over one's violations could reduce stakeholder anger as well as mitigate organization's reputation damage (Pace, Fediuk, & Botero, 2010). Besides expressing the violator's negative feelings, an apology that includes sympathy expression could help to gain favorable public responses (Chung & Lee, 2017).

Apologies can be used to reflect an organization's ethical domain that could help to restore organizational image and organization-public relationship (Ho, 2005). An effective corporate apology should indicate organization's move toward rehabilitation and its commitment on preventing similar transgression in the future (Pfarrer et al., 2008). Coombs and Holladay (2008) found that apology is not the best strategy as people reacted similarly to any victim-centered/accommodative strategy. Yet, public responses may vary depending on the components included in an apology.

Understanding what apologies can and cannot do help crisis managers to determine whether a misstep or incident merits an apology. Schweitzer, Brooks, and Galinsky (2015) outlined four considerations if an apology is necessary to avoid stonewalling or unnecessary contrition. First, considering the extent to which the organization is responsible for the occurrence of an incident or violation. Second, a violation of an organization's core business activities (i.e., hygiene issues in restaurant industry, or drivers' safety issue in auto manufacturing) requires a robust apology. Third, gauging the probable public reactions to an incident is a critical factor to determine if an apology is required. Finally, an effective organizational apology requires a commitment to implement changes in order to prevent a recurrence (Schewitzer et al., 2015). These factors contribute to crisis managers' decision-making process of crisis responses, such as to what extent organizations should take responsibility and what alternative options could be used, which is also known as strategic ambiguity (Eisenberg, 1984).

Finally, trust is commonly acknowledged as one of the key factors in interpersonal or organization-public relationships. Violations of trust occur when an organization fails to fulfill commitments, expectations, promises, or is involved in erroneous or deceptive communications (Lewicki, Polin, & Lount, 2016). Apologies following some form of trust violations can affect stakeholders' judgment toward an organization. In a trust violation, apologies were more effective than no apologies (Lewicki, Polin, & Lount, 2016). Apologies following trust violation were effective in isolated events rather than in frequently recurring problems (e.g., Kramer & Lewicki, 2010; van Laer & de Ruyter, 2010). In other words, apologies without taking lessons and acting on preventing similar violations to happen again will reduce the efficacy of apologies.

SCCT recommends crisis managers to issue an apology when there is high perception of organizational responsibility. Yet, a simple offer of apology may not generate much protection on corporate reputation damage (Pace et al., 2010). An explicit responsible acceptance should be made when the crisis responsibility is clear to be attributed to an organization, while a simple offer of apology may not be perceived as an implicit responsibility acceptance (Pace et al., 2010). Apologetic statements can generate different interpretations on responsibility acceptance and sympathetic expression.

Best practices in using apologies. An appropriate apology could help an organization to regain control of the situation and generate favorable public reactions. Domino's Pizza social media crisis response in April 2009 was a good example of using an apology (Clifford, 2009). The crisis went viral from a YouTube video uploaded by two Domino's employees in Conover, North Carolina showing themselves doing disgusting things to a sandwich before it went out on delivery. Although Domino's Pizza immediately investigated the incident internally, the organization did not publicly inform the on-going investigation. However, when the video went viral, Domino's quickly posted an apology on Twitter, then released an official statement claiming the video offensive, expressing sincerity, presenting their serious actions on correcting and assuring the issue would not happen again (Park, Cha, Kim, & Jeong, 2012). Domino's president, Patrick Doyle, also issued a response video. The company later implemented a "we suck" campaign than rebranded the company, resulting in an increase of up to 16.6 percent of sales for the first six months of 2010 (Edwards, 2010).

Consequences for not apologizing when the organization should apologize. Existing studies of apologies in crisis communications focused on examining the effects of apology and apologetic components on various variables. Although many case studies examined worst practices when organizations failed to address crises appropriately, very few studies studied the consequences or what could happen when an organization chose not to apologize when it should (e.g., Schweitzer, Brooks, & Galinsky, 2015; Thomas & Millar, 2008).

Failing to apologize may convey an idea that the transgression was done intentionally or the transgressor has yet to acknowledge the harm has been done (Thomas & Millar, 2008). Thomas and Millar's study (2008) reported that failing to apologize resulted in more anger than no communication. Participants who have low need-for-cognition trait were found to be more angry when an individual failed to apologize or did not communicate (Thomas & Muller, 2008). High need-for-cognition trait refers to individuals who engage in elaborative thinking and actively utilize information (Kardash & Noel, 2000). People who have low need-for-cognition trait do not enjoy effortful cognitive activity and tend to rely on low effort judgmental strategies or simple heuristic cues to make judgments (Cacioppo et al., 1996). Thus, an appropriate apology should convey sincerity and address stakeholders' concerns. Crisis managers may consider whether their key stakeholders are more likely to have high need-for-cognition or not in order to respond to crisis incidents effectively.

When an organization's leaders choose not to apologize in a crisis, they tend to wait, keep a low profile, argue the facts, or take a defensive stance. Reasons for not apologizing when in need could be the fear of causing bad outcomes (e.g., attract more public attention, potential trouble in legal courts), the hope that the issue would fade away from attention, or the organization's belief it has been unfairly blamed (Schweitzer, Brooks, and Galinsky, 2015), or cultural differences (e.g., publics living in countries that are high in uncertainty avoidance and power distance tend to react more strongly and quickly, to perceived threats) (Taylor, 1999). Failing to respond to a crisis with an appropriate apology could damage the organization-public relationships. For example, Coca Cola did not apologize and recall their products in Belgium when health issues happened to six kids after drinking the company's beverage in June 1999 (CNNMoney, 1999). Not until the Belgian government ordered a ban on sale of all Coke products did Coca Cola apologize and recall their products. Their poor handling of the crisis damaged the organization-public relationships and affected their sales volume significantly (CNNMoney, 1999).

Failing to apologize appropriately could cause consequences to an organization's business performance (e.g., revenue shrinking, law suits, losing customers and market share value), especially when public outcry on social media can escalate the severity of a crisis. A crisis happened with United Airlines in April 2017 when a United Airlines passenger was dragged off an overbooked flight (Victor & Stevens, 2017). United Airlines's CEO apologized for "re-accommodation" and attempted to make the problem go away by shifting the blame to a belligerent passenger and law enforcement issue (McCann, 2017). The public criticized their crisis responses on social media, called for boycott, and some even posted photos of their United Airlines credit cards being cut (McCann, 2017).

Verhoeven, van Hoof, Keurs, and Vuuren (2012) found that making apologies or not did not significantly affect individuals' perceptions on organizational reputation and their trust in the organization. However, the control message (no apology) in their experimental study included an expression of regret (Verhoeven et al., 2012). Expression of regret was considered as one of components of an apology in many studies (Bisel & Messersmith, 2012; Lazare, 2004; Pace et al., 2012; Scher & Danley, 1997; Tavuchi, 1991). Thus, it is crucial to identify what components should be included in an apology.

Apology strategy in data breach crises. Existing crisis communication studies have been focused on studying crisis communication strategies that include actual verbal and nonverbal crisis responses. Content analysis of data breach crisis communications primarily examined the content of data breach notifications (e.g., Jenkins et al., 2014; Bentley et al., 2018) or news stories covered data breaches (Kim, Johnson, & Park, 2017). Several studies of data breach crises were conducted using experimental design (e.g., Bentley, 2014, 2018).

Studies of apologies tailored into two major directions: (1) words (e.g., acknowledge, admit, regret, promise, explain) or (2) words and behaviors that including actions such as promise of corrective actions, compensations (e.g., close the access point to breached database, investigate the incident, offer customers free credit monitoring and identity theft protection in the aftermath of a data breach incident) (Bentley, 2014). Bentley (2014) also argued that a good apology should involve "a combination of words and behaviors to fix problems and rebuild relationships" (p. 21). While acknowledging responsibility, explaining the situation, urging customers to take actions to protect themselves and providing corrective actions (e.g., offering free credit monitoring) were intended to fix the problem, expressing remorse, identifying with stakeholders, requesting another chance, providing compensation (e.g., offering a coupon), and fostering personal communication (e.g., inviting contact with customer services) were meant to rebuild organization-public relationships (Bentley, 2014).

However, these two approaches lead to a question: if a good apology should include words and actions to fix the problem and/or rebuild the relationship, is it considered an apology or a combination of crisis communication strategies that are noted in a notification letter? SCCT suggests crisis managers to use several crisis strategies to respond to a situation (Coombs, 2007), such as rebuild strategies (e.g., compensation, apologies) that were categorized in preventable crises when the organization was attributed the strongest level of responsibility. Thus, it is crucial to clarify whether a good apology should include words and corrective actions or a good apology should be combined with other crisis communication strategies (e.g., corrective actions) to generate best crisis communication outcomes. Including words and actions in an apology could enhance its effects on gaining favorable public responses since having more components was found to be more efficacious than fewer components (Lewicki et al., 2016). Yet, certain components were more effective than others due to various contributing factors (Lewicki et al., 2016). Also, under potential legal and financial constraints, crisis managers consider risks and rewards associated with crisis response strategies to choose appropriate crisis one(s). Researcher argued that using words and behaviors, which was suggested in Bentley's study (2014), could be considered as apologies and corrective actions strategies. This study focused on examining the effects of apologies that using words, and referred to behaviors as corrective actions, which is one of crisis communication strategies.

Although scholars investigated apology components in many ways, a complete apology should include a responsible statement, sympathetic expression, compensation offer, and appropriate assurance that the transgression will not happen again. First, accepting responsibility should aim to reduce victims' anger, otherwise it would be more harmful than not saying apology (Coombs & Holladay, 2008; Lazare, 2004). Second, expressing sympathy could be considered as an alternative option for not accepting responsibility (Coombs & Holladay, 2008). Coombs and Holladay (2008) found that a sympathetic expression had equivalent effect compared with a responsible statement. Yet, their study did not consider the impact of causal attribution in different crisis situations. Sympathetic expression could be used when the crisis responsibility is mild (Bennett & Earwalker, 2001). When the attribution of crisis responsibility is high, only expressing sympathy without acknowledging responsibility may indicate that the organization denies its responsibility or causing ambiguity. Third, offering compensation along with taking responsibility in an apology can enhance the effectiveness of crisis responses (Courtright & Hearit, 2002). Offering compensation indicates organization's willingness to compensate or reduce the consequences of the transgression, thereby, it could help to reduce public anger. Although researcher acknowledged the important of correction actions (i.e., compensation), this study did not examine the effects of corrective actions in crisis responses. Finally, an assurance statement regarding the efforts to prevent similar future crises could represent responsible attitude of an organization, thus, foster positive public responses (Lee, 2004).

Organizations are more likely to acknowledge responsibility and express empathy when they are clearly to be blamed over data breach incidents, invite affected customers to contact with customer services and instruct them to take actions to protect themselves (Bentley, Oostman, & Shah, 2018). Although an organization and its customers are victims of a data breach, the cause of a crisis either unintentional or intentional, could significantly affect individuals' attribution to organization's crisis responsibility. Apology strategies should choose appropriate words to gain favorable public responses. Moreover, ethical reasoning approach posits that organizations should not only comply with laws and other regulations, but also create a culture of integrity based upon a concern for the law and organization's managerial responsibility on privacy issues (Culman & Williams, 2009).

Apologies are important in restoring trust in organization-public relationships. An apology should address major stakeholders' concerns. Apologies have been operationalized with multiple components (e.g., responsibility acceptance, regret expression, promise of corrective action), thus the impacts of an apology in crisis communications efforts might have divergent results across studies. Yet, what constitutes an efficacious apology and what apologetic components should be included in different trust violations must be considered. The consequence of a transgression is one of important factors to consider on what components should be included in an apology (Darby & Schlenker, 1989). Yet, if an organization's apology does not include proper components, stakeholders may perceive the apology to be insincere. An apology in a crisis situation is viewed as sincere if its components include responsible acceptance and sympathetic expression (Nadler & Liviatan, 2006; Robbernnolt, 2003). Studying the structural components of apologies in trust violation context, Lewicki, Polin, and Lount (2016) found while acknowledgement of responsibility was found to be the most important component, offer of repair and declaration of repentance were tied for most efficacious (Lewicki et al., 2016). Yet, Lewicki et al.'s study did not account for causal attribution, the level of explicitness of apology components, and the extent to which a sympathetic expression should be made. Thus, this study examined apology components, specifically responsibility acceptance and sympathetic expression in consideration of causal attribution conditions.

Causal Attribution

Causal attribution was first discussed in attribution theory, proposed by Heider (1958) and developed by Weiner and colleagues (Weiner, 1974, 1986). Attribution theory studies how individuals interpret events and how their thinking relates to their behavior. Heider (1958) argued that individuals try to understand other people's behavior by making their own judgment based on available information in order to attribute one or more causes to that behavior. The basic assumption of attribution theory is that a person will try to determine why others do what they do in order to attribute causes to an event or behavior (Weiner, 1986). Heider (1985) suggested that a person can attribute internal and/or external cause to an individual's behavior. *Internal attribution* explains that a person or organization behaves in a certain way due to something about himself/herself/itself, such as attitude, character or personality. *External attribution* infers a person's or organzation's behavior being affected by something from his/her/its situation. In a crisis, internal attribution can arise from an organization's management failure (e.g., a food contamination occurred when a restaurant did not follow food safety procedures), and external attribution can be inferred from external factors (e.g., food contamination at a restaurant occurred due to a contaminated ingredient supplied by a third party).

According to Weiner (1985), people are likely to make causal attribution when an unexpected, negative incident occurs. Individuals' attribution of crisis responsibility can affect their cognition toward an organization (e.g., Choi & Lin, 2009; Lee & Chung, 2017). Although initial crisis responsibility, crisis history, and prior organizational reputation can affect individuals’ judgment toward an organization, the level of crisis responsibility serves as a key indicator for the potential damage to corporate reputation in the wake of a crisis (Coombs, 2007; Coombs & Schmidt, 2000).

SCCT identified three crisis clusters as being victim, accidental, and preventable crises (Coombs, 2007). While data breaches can be classified into victim-crisis cluster because organizations are the victims of hackers attacking their databases the organizations appear to breach customer trust when they fail to keep their customers’ personally identifiable information secure (Bentley, 2014). Stakeholders may interpret data breaches as being accidental or preventable crisis types depending on whether organizations establish a secure infrastructure and maintain monitoring activities to protect their databases filled with customer data. In other words, the locus and controllability factors could affect individuals’ judgment on crisis responsibility toward the organization.

Causal attribution affects an organization’s decision on the extent to which it takes responsibility over a crisis. Matching crisis type and crisis responses in consideration of causal attribution is more likely to generate positive perceptions than no-response or mismatched crisis responses (Coombs & Holladay, 1996). Also, SCCT recommended that an apology with responsibility acceptance should match the responsibility that organization takes or is attributed for a crisis (Coombs & Holladay, 2002).

Accepting Responsibility

Accepting responsibility is considered the centerpiece of an apology (e.g., Coombs & Holladay, 2008; Fuchs-Bunett, 2002). Although responsibility statements are often included in organizations’ apologies, legal experts are often concerned with its potential legal consequences. Existing studies found that accepting responsibility can lower settlements (Patel & Reinsch, 2003), retain purchasing behavior and investment (Lyon & Cameron, 2004), reduce stakeholders' anger (e.g., Chung & Lee, 2017; Pace, Fediuk, & Botero, 2010), gain positive individuals' perceptions of corporate ethics (Schlenker & Darby, 1981) and integrity (Ferrin et al., 2007), increase public trust in the organization (Tomilson et al., 2004), and have better views of corporate reputation (e.g., Chung & Lee, 2017; Coombs & Holladay, 2008; Pace et al., 2010; Robbennolts, 2003). Yet, an organization's apology statement is assumed to imply responsibility acceptance, which can lead to lawsuits along with financial and reputational consequences (Pace et al., 2010). Thus, avoiding apologizing is recommended when the evidence of a transgression or responsibility is ambiguous (Patel & Reinsch, 2003).

Accepting responsibility and legal constrain. Legal experts are concerned that accepting responsibility could create a liability for the organization (e.g., Cohen, 1999; Coombs & Holladay, 2008). Patel and Reinsch (2003) argue that an appropriately worded apology does not usually create legal liability instead it could help to generate favorable public perceptions about the situation and the organization, as well as rebuild organization-public relationships. Accepting responsibility shows organization's awareness of social norms that require apologies for transgressions, reduce the uncertainty of the situation, and present the organization's morality (Robbennolt, 2003). Although apologies were found to reduce stakeholders' anger or the likelihood of a lawsuit, apologies do not help the organization to avoid punishment for transgression (Pantel & Reinsch, 2003).

Responsibility acceptance generally was operationalized in two ways. First, responsibility acceptance was operationalized as active or passive. An active responsibility acceptance clearly admits organization's responsibility over the incident (i.e., I'm sorry for hurting you) (Cohen, 1999; Lee & Chung, 2012). In contrast, a passive responsibility indirectly admits organization's responsibility, but expresses concerns arising from the incident (i.e., I'm sorry you were hurt) (Cohen, 1999; Lee & Chung, 2012). Lee and Chung (2012) found that an apology statement with active responsibility admittance generated greater public anger relief than that of passive responsibility admittance. While active responsibility acceptance reduced victims' negative feelings, passive responsibility was found to yield no effect on victims' negative feeling when the responsibility is clear (Robbennolt, 2004). Yet, passive responsibility showed positive impacts on victims' perception when the responsibility is ambiguous (Robbennolt, 2003).

Second, responsibility acceptance was operationalized as explicit (i.e., We are truly sorry and take full responsibility for the [incident], implicit (i.e., We apologize for [the incident] and we are conducting a detailed review of [the incident]), or none, which does not include responsibility acceptance or an offer of apology (Pace et al., 2010). There is a difference in perception of responsibility between an offer of apology (implicit statement of responsibility acceptance) and an apology with an explicit statement of responsibility acceptance (Pace et al., 2010). The extent to which stakeholders attribute crisis responsibility toward an organization could affect the organization's decision on whether an apology should be made. Thus, crisis managers not only consider potential legal liabilities, but also attempt to reduce victims' anger when choosing crisis response strategies. An explicit responsible apology should be made along with affirmative steps to repair damage when the transgression is inevitable. Yet, an implicit responsible acceptance is more likely to cause no effect or resolve the problem when the transgression is clear (Patel & Reinsch, 2003).

Responsibility acceptance and sympathetic expression in apologies were found to have no different effects on individuals' anger or negative word-of-mouth (Coombs & Holladay, 2008; Choi & Lin, 2009). Yet, these studies did not consider causal attribution of the crisis, which could affect individuals' judgment on the level of the organization's crisis responsibility. In data breach crises, the types of personally identifiable information could affect individuals' judgment toward crisis responsibility because important information, such as credit or debit cards, requires affected individuals to take actions immediately to prevent potential damage. Thus, individuals may attribute higher level of crisis responsibility toward the breached organization.

Apologetic responses were more effective than defensive responses at creating positive customer impressions toward an organization and motivating them to do business transactions with the organization (Lyon & Cameron, 2004). Yet, how stakeholders interpret the meanings of apologies and how they attribute crisis responsibility can affect the effectiveness of crisis responses. Accepting responsibility was also found to increase forgiveness and sympathy toward the organization (Weiner, Graham, Peter, & Zmuidinas, 1991). Although apologies were found to be no more effective at improving attitudes toward an organization than offering compensation or expressing sympathy in Coombs and Holladay's study (2008), sympathetic expression toward victims could contribute to yielding favorable public responses.

Expression of Sympathy

Sympathetic expression could make apologies be more effective (e.g., Patel & Reinsch, 2003). Expressing sympathy to stakeholders who are directly or indirectly suffering from the wrongdoing enables the organization to ask for forgiveness of the wrongful actions and seek reconciliation (Frandsen & Johansen, 2010). Apologies with sympathetic expressions could contribute to resolve the problem or rebuild the relationships between the victims and an organization (Patel & Reinsch, 2003). By focusing on the victims' situation/suffering as well as disclosing all relevant information of the wrongdoing (except discretion), an organization shows its moral practices that could make the apologies sincere (Weiner, 1985). Thereby, apologies with sympathetic expressions could make the statement more effective. Through the legal lenses, sympathetic expression is viewed as a safe choice in crisis responses. An apology with a sympathetic expression was found to not increase the likelihood of a lawsuit or to be interpreted as a responsible acceptance by judges and jurors (Myers, 2016; Robbennolt, 2003). Thus, sympathetic expression in an apology statement could reduce legal concerns.

Sympathetic messages expressing the organization's sincere and empathetic apologies could reduce public anger (Byrne et al., 2014; Englehardt, Sallot, & Springston, 2004; Grappi & Romani, 2015; Robbennolt, 2003). Sympathetic expression was considered as highly accommodative strategies through the focus on victims' needs that helps to rebuild the relationships with public (Coombs, 2006; Coombs & Holladay, 2008; Diers-Lawson & Pang, 2016; Fediuk, 2002; Sturges, 1994). A statement of sympathy and a statement of responsibility were found to have equivalent effect on crisis responses (Coombs & Holladay, 2008). Yet, stakeholders tend to expect a statement of responsibility acceptance in severe crises. In order words, the crisis type(s) used in an experimental study could affect the findings of individuals' reactions.

An immediate sympathetic expression in a statement issued right after a crisis situation could help to reduce tensions between parties involved and mitigate the threat of a potential lawsuit (McCullough, Worthington, & Rachal, 1997). Although an apology with sympathetic expression may not suffice, a sincere sympathetic expression could contribute to relieving individuals' anger to a certain extent (Chung, 2011). McCullough et al. (1997) contended that people who perceived the sincerity of an apology with sympathetic expression are more likely to forgive a transgression. Expressing sympathy shows the organization's concerns on victims' unfortunate situation and a care for public safety as a priority in crisis responses (Coombs, 2007). Thus, issuing an apology statement with a sympathetic expression could effectively reduce public's anger. Yet, different level of a sympathetic expression could yield different public responses.

Existing studies examined an expression of sympathy based on (1) the explicitness or (2) the level of sympathy. First, sympathetic expression was operationalized in two levels of sympathy: explicit sympathetic expression versus none. A statement of explicit sympathetic expression shows empathetic feeling toward people who are suffering from the situation (Chung & Lee, 2017). The *none* condition did not include any sympathetic expression in the apology statement. Second, the level of sympathy: high versus low. The high level of sympathy referred to the organization's empathetic feeling toward the victim affected by the crisis situation, which is similar to the operationalization of an explicit sympathetic expression. Meanwhile, the low level of sympathetic expression referred to the organization's awareness and understanding to the people affected by a crisis (Chung, 2011).

Public Anger

Anger has been studied in various emotion theories (e.g., James-Lange theory of emotion, Cannon-Bard theory of emotion, Schachter-Singer's two-factor theory of emotion, Lazarus' cognitive mediational theory). James-Lange theory posits that the stimulus leads to physiological arousal that instigates the experience of emotion (Walter, 1927). On the other hand, the Cannon-Bard theory argues that the stimulus leads to both arousal and emotion. In other words, physiological arousal does not have to occur before emotion (Walter, 1987). Arousal and feeling emotion, in response to a stimulus, are independent. Magda Arnold (1960) advanced appraisal theory of emotions by shifting the emphasis of studying emotions from “feeling” theories and “behaviorist” theories to cognitive approaches, which now dominates current studies in the field.

From the cognitive approaches, Schachter and Singer’s two-factor theory posits that stimulus leads to arousal that is labeled using cognition that leads to emotion. Anger is an experienced emotion based on the situational appraisal of the experienced physiological arousal (Lazarus, 1991). The stimulus leads to personal meaning derived from cognition, which leads to both arousal and emotion (Lazarus, 1991).

Anger was found to be the most influential and strongest emotion in a crisis (e.g., Choi & Lin, 2009). The causes of a crisis situation affect individuals’ judgment on the actor that is responsible for the crisis (Coombs & Holladay, 2007; McDonald et al., 2010). Anger and negative attitudes toward an organization could be elicited when stakeholders attributed responsibility to the organization (Coombs & Holladay, 2007). Thus, crisis responses should aim to reduce stakeholders’ anger.

The feeling of anger may affect individuals’ reactions to an incident such as resentment cognition (Novaco, 1994) or the feeling of annoyance or rage (Allocorn, 1994). Various factors such as physical or psychological restraint, perceptions of being unfairly slighted, or disgust with others’ behavior could trigger anger (Izard, 1991; Lazarus, 1991). People tend to stay emotion-focused about their anger instead of triggering anger relief (Lerner, 1990; Mitchell, Brown, Morris-Villagran, & Villagran, 2001; Smith & Dillard, 1997). In other words, people are more likely to focus on emotionally relevant thoughts of a persuasive message.

The extent to which individuals believe a crisis was caused by an organization affects individuals’ attribution of crisis responsibility (Weiner, 1985) and their affective responses toward the organization (e.g., Coombs, 2007; McDonald et al., 2010). Anger was found to elicit when individuals' attribute crisis responsibility to the organization (e.g., Coombs, 2007; Chung & Lee, 2017). When the causes of a crisis can be identified, it helps individuals to determine whether organizations are victims, or if the organizations' actions were unintentional or intentional (Coombs, 2007). Although both organization and their customers are victims in a data breach crisis, the organization's failure to protect customers' personally identifiable information could trigger public anger.

Anger often leads to negative consequences. Anger can motivate people to express negative attitudes toward an organization that could damage organizational reputation, or even cease the organization-public relationships (Jorgensen, 1996; Stockmyer, 1996). Individuals' anger can create negative word-of-mouth about the organization, reduce purchase intentions (Coombs & Holladay, 2007) and investment intentions (Jorgensen, 1996). Thus, apologies should be made appropriately to reduce public anger.

Organizational Reputation

Based on the aggregated evaluation of the extent to which an organization's past behaviors meet stakeholder's expectations, stakeholders form perceptions, either favorable or unfavorable, toward organizational reputation (Wartick, 1992). Stakeholders receive information about an organization in various ways, such as interactions with the organization (i.e., purchasing and consuming products or services, interacting with customer services), mediated reports (i.e., advertising, media coverage about the organization), and second-hand information sources (i.e., word-of-mouth, blogs) (Coombs, 2007). This information provides input for stakeholders to compare what they know about an organization and how well the organization meets their expectations to form perceptions of the organizational reputation. Since organizational reputation, as a valued resource, is threatened by crises, strategic crisis responses have a significant impact on the outcomes of a crisis, including protecting affected stakeholders and the amount of reputational damage sustained by the organization (Coombs, 2007, 2010). Since the crisis response strategies should be chosen based on the consideration of crisis responsibility attribution and reputational threats posed by a crisis, strategic responses should aim for restoring organizational reputation.

The more severe stakeholders judge a crisis incident, the more they perceive organizational reputation negatively (Claye et al., 2010; Coombs, 1998; Coombs & Holladay, 2002). Rebuild strategy, such as apologies, leads to the most positive reputational restoration (Claeys et al., 2010). However, people with an external locus of control prefer the use of *deny* strategies than those with an internal locus of control (Claeys et al., 2010). Similarly, when an organization believes that an external factor causes an incident more that the organization's actions itself, the organization may choose to reject responsibility for what happened by using deny strategies.

The majority of existing studies and theories in crisis communication research focus on theorizing and measuring the effectiveness of crisis communication responses in repairing organizational image and/or restoring organizational reputation (e.g., Benoit, 1995, 1997, 2015; Coombs, 2007). Managers attempt to generate sufficient understanding or solve conflict so the stakeholders or community can judge and react to organizational crisis responses. Outcome assessment of crisis responses include image and reputation restoration, issues development, improvement on risk management, legitimacy, organization-public relationships quality, uncertainty reduction, stakeholder exchange, understanding, and agreement (Heath, 2010). Although reputation management or image restoration is considered to be an organizational outcome variable, very few studies factored in the relations between trust in crisis communications and organizational reputation.

Some argued that trust is an outcome of favorable organizational reputation (e.g., Keh & Xue, 2009), while others argued that trust in organization affects perception on organizational reputation (e.g., Yoon et al., 2006; Walsh et al., 2009). This study posits that trust is an antecedent to organizational reputation. Trust is a cognitive construct, while organizational reputation is an affective construct that affect individuals' attitude toward an organization (Fazio, 1986). Individuals' judgment or attitude toward an organization can be formulated based on individuals' knowledge or beliefs toward an organization (Fishbein & Ajzen, 1975). In a data breach context, this study examined the effects of apologies on individuals' trust in organization (cognitive aspect) and organizational reputation (affective aspect). Apologies are delivered consistently to demonstrate organizational values that align with societal and ethical values that are critical to build an organization's image and trustworthiness (van der Mere & Puth, 2014).

Trust in Crisis Communications

Trust refers to "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, p. 712). Trust in an organization refers to stakeholders' judgment of how much they feel they could trust the organization (Lee, 2005, p. 108). In a data breach context, this definition of trust is applicable because it helps to explain why stakeholders (trustor) give a greater or lesser amount of trust to an organization (trustee) depending on stakeholders' expectation about the organization in fulfilling what it claimed or promised to do. One approach to understanding trust is to consider attributes of the trustee that help the trustor determines if the trustee is trustworthy (Hovland, Janis, & Kelley, 1953; Mayer et al., 1995). In other words, trustworthiness is a multifactor construct and serves as an antecedent of trust.

Studies also found other trust antecedents, including transparent communication (Auger, 2014), message congruency (Mejinders et al., 2009), or willingness to share personal information (Blancharel et al., 2011). Trust consequences were found in various studies, such as behavioral intentions (Auger, 2014; Cleeren et al., 2008; DiStaso et al., 2015; Spence et al., 2016), subsequent information searching (Ruppel, 2016), and blame or performance evaluations (Griffin et al., 2008). Yet, it remains unclear: (a) which trust antecedents have significant relationships with trust, (b) the role of trust on behavioral outcomes (Colquitt, Scott, & LePine, 2007), and (c) whether trust is an antecedent or outcome of organizational reputation.

Trustworthiness is a unidimensional variable and one of the most important aspects of an organization's reputation (Coombs & Holladay, 2002). Trustworthiness is commonly used in reputational measures, including the most popular one—the reputational quotient developed by Fombrun (1996). Fombrun's reputation quotient measures stakeholders' perceptions of an organization's reputation as well as compares organization' reputation both within and across industries. The quotient includes 20 attributes divided into six groups: emotional appeal, products and services, vision and leadership, workplace environment, financial performance, and social responsibility. Since trustworthiness is the central of the trust concept, this study focused on examining the effects of causal attribution and apologetic components on trust in organization's competence, integrity, and benevolence. This study uses these three variables of trustworthiness developed by Mayer, Davis, and Schoorman (1995), that has been used in various studies (e.g., Colquitt et al., 2007; Mayer & Davis, 1999; Park, Lee, & Kim, 2013) to examine trust in an organization.

Some viewed trust as synonymous with trustworthiness in which individuals (trustors) have positive expectations on other individuals (trustees) based on trustees' personal characteristics (e.g., McKnight et al., 1998). Others argued that trust is based on three characteristics, including competence, benevolence, and integrity, which comprise trustworthiness of an individual or organization (Mayer & Davis, 2007; Mayer et al., 1995). Trustworthiness is used to evaluate an individual or organization's characteristics and actions that lead to trust (Mayer et al., 1995).

Three components that appear to explain a major portion of trustworthiness include: competence or ability, benevolence, and integrity (Mayer et al., 1995). *Competence* (also known as *ability)* refers to knowledge, skills needed to perform a specific job, interpersonal skills, and general wisdom to succeed in the workplace (Gabarro, 1978). *Benevolence* refers to the extent to which a trustee is believed to behave well with a trustor, aside from profit motives, such as loyalty, caring (Mayer et al., 1995). *Integrity* refers to the extent to which a trustee is believed to follow moral and ethical principles to maintain fairness and justice (Colquitt, Scott, & LePine, 2007; Mayer et al., 1995; Tomlinson & Mryer, 2009). While *competence* emphasizes the knowledge and skills of the trustee to perform a certain task, *benevolence and integrity* describe whether the trustee will use knowledge and skills to act on the trustor's interest (Colquitt et al.; Campell, 1990). Benevolence captures emotional connections with the trustee with the positive impact of caring and supportiveness (Lind, 2001). In contrast, the integrity factor features sound moral and ethical principles that describe the rational reasons for an individual to deal with uncertainty and the means to establish trust in someone (Lind, 2001). Consumers may react negatively to a crisis incident if they attribute high crisis responsibility toward an organization.

Crisis communications should attempt to attain organizational reputation and being perceived to behave well in their responsibility. This effort can impact trust in organization.

Trust in an organization's competence, integrity, and benevolence varies depending on the nature of violations or context. Lewicki, Polin, and Lount Jr (2016) found that apologies including more components, specifically in competence- and integrity-based offenses, were more effective than those with fewer components. Certain apologetic components are more important than others, but its efficacy is affected to some degree by the context of an apology and the number of components aggregated in the apology (Lewick et al., 2016). Three components should be used in a single apology, including an explanation for why the violation occurred, offer of repair for economic damage, and acknowledgement of responsibility for having created the violation (Lewicki et al, 2016). Apologies with competence-based offenses were found to be more effective than those with integrity-based offenses (Lewicki et al, 2016; Kim et al., 2004).

Trust in organization's competence. Trust in competence is domain specific as the trustee should have knowledge, skills, and characteristics in some specific areas that earned people trust on them in performing tasks related to those areas (Mayer et al, 1995; Zand, 1972). Consumers learn from an organization's competence from the use of its products and services, mass media, or third-party information sources (e.g., word-of-mouth). Perceived competence leads to certain expectations toward the organization, that subsequently develops consumers' trust in organization's competence. In the data breach crisis communication context, individuals judge organization's competence on its skills and knowledge to perform actions in order to handle the situation as claimed in the notification letter. Since data breach notification is the primary and direct communication from the organization to its customers, this is often how customers learn about the cause of the crisis that enables them to attribute crisis responsibility.

Trust and organization's benevolence. Benevolence is the perception of trustee's positive orientation toward the trustor (Mayer et al., 1995). Thus, perceived benevolence plays an important role in assessing if an organization is trustworthy. Stakeholders' trust can develop through emotional bonds with the organization, that in turn enhance affective bonds and interactions with the organization (Williams, 2001).

Trust in an organization's integrity: Stakeholders build their trust in an organization's integrity based on the consistency between the organization's values and its behavior, and whether the organization adheres to principles of fairness (Mayer et al., 1995). Trust in integrity could be based on the consideration if the organization fulfills legal and ethical responsibilities. Notifying customers about a data breach incident not only shows that the organization comply with pertinent regulations, but also reflects that the organization concerns about its customers' wellbeing. Once customers perceive that the organization was honest and fair to them in providing sufficient information, they are more likely to trust the organization (Elkins, 1976).

Trust is a critical factor in organization-public relationships (Hon & Grunig, 1999) as well as having certain roles in building and maintaining corporate reputation. When stakeholders attribute crisis responsibility to an organization, the organization might have broken stakeholders' trust by doing or saying something wrong. Thus, crisis responses should aim to not only fix the issue, but also repair broken trust when an organization failed to meet stakeholders' expectations (Falkheimer & Heide, 2015). Although major research in crisis communications acknowledged reputational threats inflicted in a crisis, very few studies examined trust in crisis communications and reputation management (e.g., Coombs & Holladay, 2002; DiStaso, Vafeiadis, & Amaral, 2015; Freimuth, Musa, Hilyard, Quinn, & Kim, 2014; Hon & Grunig, 1999; Meredith, Eisenman, Rhodes, Ryan, & Long, 2007). Trust in crisis communication research was treated differently. DiStaso et al. (2015) measured reputation and trust outcomes from crisis responses in which trust was evaluated using three dimensions, namely, integrity, competence, and dependability. Different trust components were also examined at different crisis stages (Freimuth et al, 2014; Meredith et al., 2007). Yet, existing studies fell short of going beyond traditional crisis response strategies to rebuild trust or examine the relations of trust and organizational reputation.

Main Effects of Causal Attribution, Responsibility Acceptance, and Sympathetic Expression on Public Responses

Causal attribution. The cause of a crisis affects individuals' judgment and reaction to an organizational transgression. Anger is a common reaction toward an actor or organization that is blamed over an incident, particularly, when a high level of responsibility is attributed (Boston et al., 2007; Darley & Pittman, 2003; Weiner, 2004). Negative emotions toward the organization, such as anger, are more likely to form when stakeholders attribute internal and controllable cause of an incident than those of external and uncontrollable reasons (Lee, 2004; Weiner, 1985). Additionally, apologies for a transgression that is tied to an external/uncontrollable factor tend to gain individuals' acceptance and forgiveness (e.g., May & Jones, 2007; Takuku, 2001).

The effects of reputation damage (e.g., a reduction in revenue or market share value, expenses on compensation for injury) is expected to be more severe in a high level of attributed responsibility than those of low attributed responsibility (Pace, Fediuk, & Botero, 2010). The more people attribute crisis responsibility toward an organization, the more likely people perceive organization's reputation negatively (Coombs & Holladay, 2002; Coombs, 2007). Moreover, under internal/controllable crisis situations, people tend to question an organization's competence that relates to knowledge, skills and characteristics (competence) to handle certain situations or tasks. Thus, people may trust the organization’s competence when they perceived a crisis was caused by external/controllable factor(s) more than the one caused by internal/controllable factor. Also, when the cause(s) of a crisis is uncontrollable or was affected by external factor(s), people may feel pity or sympathy toward the organization (Weiner, 1985). Since benevolence can be formed through individuals’ emotional bonds, which lead to their affective bonds and interaction with an organization, people tend to trust in organization’s benevolence when they perceived a crisis was caused by external/uncontrollable factor(s) more than a crisis caused by internal/controllable one(s). Finally, Kim et al. (2004) noted that apologies are more effective in competence-based offenses than they are in integrity-based offenses. If an organization chooses to reveal the cause(s) of a crisis, people may perceive the organization’s behavior(s) as being transparent and adhering to ethical principles (integrity). Thus, this study predicted that individuals’ trust in an organization’s integrity would not be different when they could know the cause(s) of a crisis as revealed in an organization’s statement. Based on these arguments, two hypotheses were proposed:

H1a: Participants who read an apology statement with an external/uncontrollable causal attribution are more likely to (a) reduce anger, (b) hold a positive perception on organizational reputation, and (c) have higher trust in an organization’s competence, and (d) benevolence than those who read an apology statement with an internal/controllable causal attribution.

H1b: Participants who read an apology statement with an external/uncontrollable causal attribution have no difference in their trust in an organization’s integrity compared to those who read an apology statement with an internal/controllable causal attribution.

Responsibility acceptance. Pace at el. (2010) found that the more an organization accepts responsibility after a transgression, the less likely stakeholders feel angry at the organization.

Thus, an explicit responsibility acceptance is more likely to reduce stakeholders' anger than an implicit responsibility acceptance (a simple offer of apology) or an apology without accepting responsibility. Moreover, the greater stakeholders feel angry at the organization, the greater the reputation damage (Pace at el., 2010). An appropriate apology could yield a more favorable impression of the offender (Ohbuchi et al., 1989). Coombs & Holladay (2008) argued that the public tend to perceive organizational reputation more positively when an organization takes responsibility for the crisis. Thus, an apology that explicitly accepts responsibility could yield more positive perceptions toward organizational reputation than an apology without explicitly taking responsibility. Accepting responsibility could help to reduce reputation damage. Moreover, despite the disagreement whether trust is an antecedent to organizational reputation or vice versa (e.g., Keh & Xue, 2009; Yoon et al., 2006), trust and reputation are relevant factors that could affect an organization business performance. When a transgression occurs, an explicit responsibility acceptance could help to rebuild public trust in an organization's competence. Accepting responsibility is an indicator that reflects the organization's commitment on ethical behaviors, makes morally right decisions, undertake activities to fulfill consumers' expectations (Frandsen & Johansen, 2010) in order to rebuild stakeholders' trust in the organization's integrity. An apology that conveys positive motives and intentions to take responsibility to fix the problem could reflect the organization's genuinely concerns with customers' wellbeing. Subsequently, it helps to rebuild customers' trust in an organization's benevolence.

H2: Participants who read an apology statement with explicit responsibility acceptance are more likely to (a) reduce anger, (b) hold a positive perception on organizational reputation, and (c) have higher trust in an organization's competence, (d) benevolence, and (e) integrity than those who read an apology statement with an implicit responsibility acceptance.

Sympathetic expression. Sympathetic expression in a statement should express concerns for victims aims to show an organization's care for the victims and ease the victims' anger (Chung, 2011). An expression of sympathy could help to reduce public anger when perceived crisis responsibility is mild (Bennett & Earwalker, 2001). However, the fictional data breach scenario used in this experimental study is a severe crisis incident which involved a large number of breached accounts of personally identifiable information, thereby, only expressing sympathy would not suffice to reduce public anger. Similarly, since there is a positive relationship between anger and reputation damage (Pace et al., 2010), researcher argues that only expressing sympathy would not help to gain favorable perception of organizational reputation. Moreover, trust in an organization's competence, which indicates the organization knowledge and skills to fix the problem, could not be formed by using a sympathetic expression in a statement. Similarly, a sympathetic expression may not yield trust in an organization's integrity which can be determined if the organization abides to its ethical principles. It is questionable whether a sympathetic expression would be sufficient to generate emotional and affective bonds (benevolence) from stakeholders toward an organization after a severe crisis. Thus, this study predicted that different levels (high vs. low) of sympathetic expression yield no different effects on public reactions.

H3: Participants who read an apology statement with high sympathetic expression have no different reactions in terms of (a) relieving anger, (b) perceiving organizational reputation, and (c) trusting in an organization's competence, benevolence compared to those who read an apology statement with low sympathetic expression.

Interactions of Causal Attribution, Responsibility Acceptance, and Sympathetic Expression on Public Responses

Causal attribution and responsibility acceptance. The cause of a crisis affects individuals' judgment and reaction to an organizational transgression. Apologies citing internal/controllable factors tend to have less favorable public responses than those citing external/uncontrollable factors (Weiner et al., 1987). When a crisis is perceived as internal/controllable, people might attribute high crisis responsibility. The more the people attributed crisis responsibility to the organization, the more likely they will elicit their anger (Pace et al., 2010). Since induced anger can facilitate individuals' active information processing (Nabi, 1999), a crisis communication message's characteristics could affect individuals' judgment on crisis responses (Chung & Lee, 2017). An apology that actively admit responsibility could contribute to reduce public anger in an internal/controllable crisis situation (Lee & Chung, 2012). Thus, an explicit responsibility acceptance might help to reduce stakeholders' anger compared with an implicit responsibility acceptance or a simple offer of apology. Additionally, the more people attribute crisis responsibility toward an organization, the more likely people perceive organizational reputation negatively (Coombs & Holladay, 2002; Coombs, 2007). When a crisis is perceived to be caused by an internal/controllable factor, an explicit responsibility acceptance could indicate the organization's commitment in taking actions to fix the issue. Thus, accepting responsibility in an internal/controllable crisis situation could help to reduce reputational damage.

Under internal/controllable causal attribution, people tend to question an organization's competence that relates to its knowledge, skills and characteristics to handle certain situations or tasks. Apologies are more effective in competence-based offenses than they are in integrity-based offenses (Kim et al., 2004). Thus, an explicit responsibility acceptance, which shows the organization’s claims or efforts to fix the issue, could help to rebuild stakeholders’ trust in the organization’s competence. Accepting responsibility is an indicator that reflects the organization’s commitment on ethical behaviors, makes morally right decisions, undertake activities to fulfill consumers’ expectations and earn back the trust in organization’s integrity. An apology that conveys positive motives and intentions to take responsibility to fix the problem could reflect the organization’s genuinely concerns with customers’ wellbeing. Subsequently, it helps to rebuild customers’ trust in an organization’s benevolence. Moreover, accepting full responsibility for a wrongdoing prevents creating an internal or external scapegoat to which the organization attempts to shift blame (Frandsen & Johansen, 2010). On the contrary, if a statement does not include a responsibility acceptance, public may view it as defensive or inadequate for crisis responses. Thus, it is hypothesized that:

H4a: Under an internal/controllable crisis situation, participants who read an explicit responsibility acceptance are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust the organization’s (c) competence, (d) integrity, and (e) benevolence than those who read an implicit responsibility acceptance.

H4b: Under an internal/controllable crisis situation, participants who read an implicit responsibility acceptance are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust the organization’s (c) competence, (d) integrity, and (e) benevolence than those who read an apology without a responsibility acceptance.

Causal attribution and sympathetic expression. Sympathetic expression shared public’s concerns and feelings which align with suggestions in Situation Crisis Communication Theory that purport that public safety should be the primary concern in crisis responses (Coombs &

Holladay, 1996, 2002). Also, high sympathetic expressions could increase the sincerity of an apology statement (Gobodo-Madikizela, 2003). Lee and Chung (2012) found that public anger relief had no different effects between high and low sympathetic expressions. Yet, when a crisis is perceived to caused by internal/uncontrollable, a high sympathetic expression could reflect the organization's regret for causing the incident and show the organization's care for victims' concerns and feelings. Thus, when public perceived a crisis was caused by an internal/controllable factor, a high sympathetic expression might help to reduce public anger and mitigate reputation damage.

Organizational apology aims to gain public sympathy toward the organization for breaking the public's trust in the organization's competence in performing certain actions. Although a high sympathetic expression could not yield significant effect on regaining the public's trust in an organization's competence, it could present the consistency between the organization's values and its behaviors, as well as reflecting the organization's genuinely concerns for public's wellbeing. Since a sympathetic expression focuses on addressing stakeholders' concerns and feelings, it may have limited effect in regaining trust in organization's competence. Thus, the hypothesis that follows did not make prediction on the effects of sympathetic expression on trust in competence:

H4c: Under an internal/controllable crisis situation, participants who read a high sympathetic expression are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust the organization's (c) benevolence and (d) integrity than those who read a low sympathetic expression.

Causal attribution, responsibility acceptance, and sympathetic expression. This study assumes that when people perceived a crisis is caused by an external/uncontrollable factor, they tend to react more positive than a crisis caused by an internal/controllable factor. Since people tend to react negatively to a crisis incident that is perceived to be caused by internal/controllable factors, people may expect an organization's apology that explicitly take responsibility with high sympathy to victims who are being affected by the crisis. A combined message of responsibility acceptance and sympathetic expression could be viewed as a full apology (Chung, 2011). Accepting full responsibility with a high sympathetic expression for a wrongdoing not only shows the sharing to stakeholders' concerns and feelings but also prevents creating an internal or external scapegoat to which the organization attempts to shift blame (Frandsen & Johansen, 2010). Thereby, under an internal/controllable crisis situation an apology with explicit responsibility acceptance and high sympathetic expression might contribute more in relieving stakeholders' anger, restoring reputation, and regaining trust in an organization than a simple apology (implicit responsibility acceptance) with a low sympathetic expression. Thus, this study predicted that:

H5: Under an internal/controllable crisis situation, participants who read an explicit responsibility acceptance and high sympathetic expression are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust in organization's (c) competence, (d) integrity, and (e) benevolence than those who read an implicit responsibility acceptance and low sympathetic expression.

Chapter 3: Methods

Justification of the Method

This study used an experimental design to draw causal conclusions, specifically, whether treatments of the three factors (independent variables) caused change(s) in outcome (dependent variables). By controlling extraneous variables, researcher can conclude whether the manipulation of independent variables causes any changes in dependent variables (Creswell, 2013). Moreover, experimental research designs allow researchers to replicate studies to check and verify studies' results (Creswell, 2013). Under the controlled environment of experimental research, researchers can tailor the experiment while he or she is still able to maintain the validity of the study design (Neuman, 2013).

Experimental research have several limitations. First, the artificial situations in experimental setting do not often represent real life. Thus, study participants' reactions may not indicate their behaviors in a non-experimental environment (Keppel, 1991). In order to reduce this disadvantage, researcher used a hypothetical company—TechBuy, that enabled participants to draw a connection or think about—BestBuy, an American multinational consumer electronics retailer. Second, although experimental research is used to ensure internal validity, external validity is an expense (Keppel, 1991). In other words, the study results may not be generalizable to a broader population. However, researchers can examine causation. Finally, although experimental research is a powerful tool for determining or verifying causation, this research method can not explain "why" the outcome occurred (Creswell, 2013; Keppel, 1991). Since this study focused on examining causation, findings and conclusions provided interpretation and possible explanation of findings. Researcher acknowledged that future studies should use other research methods (i.e., interviews) in order to specify why the outcome occurred.

This study used a between-subjects design to minimize the possibility that study participants figure out the manipulation which could affect their answers in the survey (Wimmer & Dominick, 2011). The procedures in a between-subjects design require random assignment for each participant to expose to one condition, manipulation, or treatment (Mark & Reichardt, 2004). Then, researchers compare the results across groups. A minimum of participants per group is suggested, for example, using G*power software to calculate sample size. However, statistical power analyses tend to optimize the sample size for the given or anticipated effect size in software like G*power (McCallum, Browne, & Sugawara, 1996). Comparing with within-subjects experimental design, between-subjects experimental research require more participants, resulting in more time-consuming and costly.

In contrast, each participant in a within-subjects design exposes to multiple treatments, enabling researchers to compare their results to treatments or conditions (Mark & Reichardt, 2004). Using a within-subjects design requires fewer participants and produces greater power (Wimmer & Dominick, 2011). The main advantage of a within-subjects experimental design is that internal validity does not depend on random assignment. Thus, it can reduce error variance of independent variables because each participant acts as his or her own control (Wimmer & Dominick, 2011). This study chose to use between-subjects experimental design that minimizes the possibility of study participants figuring out the manipulation (Wimmer & Dominick, 2011). It increased the chance to collect valid data.

Design

A 2 (Causal attribution: internal vs. external) x 3 (Explicitness of accepting responsibility: none, explicit, implicit) x 2 (Expression of sympathy toward victims: high vs. low) between-subjects design was used to examine the impact of causal attribution, responsibility acceptance, and sympathetic expression on public anger relief, perceived organizational reputation, and degree of trust in organization's benevolence, integrity, and competence. Experimental materials include a fictional news article about a data breach crisis scenario, apology statements in the form of a data breach notification letter, and survey questionnaires. Twelve types of statements (scenarios) were created based on the levels of each independent variable.

Stimuli

Veltsos (2012) found that data breach notifications should be written in a direct pattern which presents the bad news first and then provide information about identity protection (i.e., describe and explain the breach, organizational responses, and give directions). Apology was found as one of effective strategies in security breaches (Jenkins et al., 2014). Expressing sympathy which focuses on victims' needs could helps to rebuild the relationship with public (Coombs, 2006; Diers-Lawson & Pang, 2016; Fediuk, 2002). Thus, the stimuli included two materials: a news article and a statement in the form of a notification letter. The news article is the same in the twelve conditions. The manipulation of independent variables was shown in statements that were structured with the cause of the crisis, types of breached information as required in data breach notification state laws (e.g., 201 Code of Massachusetts Regulations 17, 2009), apology (if any), and sympathetic expression.

A hypothetical data breach crisis occurred at TechBuy—a fictional giant American consumer electronic retailer, was used to manipulate different statements. A breach could be considered as a severe incident when important personally identifiable information, such as social security number, financial record was compromised (Identity Theft Resource Center, 2017). Thus, to control the severity of a crisis, types of consumer information that was compromised, including names, mailing addresses, phone numbers or email addresses, and debit/credit cards, were used with the assumptions that they would make people not only relate to the exposure of the potential risks associated with a data breach incident, but also trigger their judgment on possible negative consequences of the incident. This study used a severe fictional data breach incident because a mild data breach, such as customers' name and email addresses were compromised or the incident that affects a small amount of customers' accounts (i.e., less than 1% total amount of customers), might not get much attention from affected individuals or being perceived as causing mild or no harm.

Causal attribution. Causal attribution was manipulated based on the reasons of the hypothetical data breach case. The reasons of the data breach scenario reflected two factors of causal attribution, including *locus of control*—whether internal or external factor(s) causes the incident, and *controllability*—whether an individual or organization involved in the incident can control the causes (e.g., skills) or cannot control it due to other factors (e.g., out of luck) (Weiner, 1986). Based on common identified reasons of a breach (i.e., unintentional leaks, illegal sales of personal information, or outright data theft) (Friedman & Telang, 2006), the message for causal attribution was manipulated. The internal/controllable condition cited unintentional leaks due to an employee/employees' negligence, while the external/uncontrollable condition was manipulated due to outright data theft with a self-defensive message ("We, TechBuy, invest $10 million every year to strengthen our cybersecurity system to keep our customers' information secure"). This study argues that regardless of how professional cyber-security teams are and how complicated the data security system are, hackers do only one job which is to find a way(s) to get access to the organization's database. Thus, outright data theft in this study was viewed as external/uncontrollable factor. Additionally, a self-defensive message before citing the external/uncontrollable cause is crucial to emphasize the efforts to protect customers' data. It also provides more information for individuals to determine if the breach was caused by an external/uncontrollable factor.

Responsibility acceptance. To examine the effect of responsibility acceptance in an organizational apology, this study used conceptual definitions of three levels of responsible acceptance that was used in Pace et al.'s study (2012): (1) explicit responsible acceptance, (2) implicit responsible acceptance, and (3) none. An explicit statement of responsible acceptance includes an apology with full responsibility acceptance ("We are truly sorry for the inconvenience this incident may cause you. We're taking this incredibly seriously and accept full responsibility to fix this security problem"), while an implicit responsible acceptance simply includes an apology ("We are truly sorry for the inconvenience this incident may cause you"). The *none* condition did not include responsibility acceptance.

Expression of sympathy. The operationalization of sympathetic expression was modified from Chung's (2011) study. The high sympathy statement elaborated the organization's sharing of victim's feelings and tried to relate the same feelings that victims might be experiencing, while the low sympathy statement simply expressed that the organization's understanding of the problem and the frustrated experience victims might have.

Conditions of the three independent variables are detailed in Appendix B. Twelve variations of organizational statements were created using different combinations of causal attribution, responsibility acceptance, and sympathy expression. Researchers acknowledged that experimental materials, including the news article, apology statements, and survey questionnaires are limited in a text format, which can affect the perceptions of recipients who tend to rely on visual image or sound to process information.

Participants

Participants were recruited on Amazon's Mechanical Turk (MTurk), a crowdsourcing Internet marketplace that allows businesses and individuals to post short tasks and pay workers. MTurk provides researchers with access to a diverse set of people making the study population more accessible and cost-effective. Rouse (2015) found that MTurk-based responses were significantly less reliable than normative or community-based samples. Rouse (2015) also reported that using questions to verify if workers were attentive and honest was associated with more reliable responses. Three verifying questions were added in different parts of the survey for quality check (e.g., for quality check, please choose "disagree" in this row). These verifying questions checked if workers paid attention to the survey or answering multiple-choice questions randomly without reading the question and/or answering options. For examine, if workers answered any options other than "disagree" in the question "For quality check, please choose "disagree" in this row," they would be unable to continue to participate in the survey. These verifying questions were deleted before analyzing data. Several parts were timing to ensure that participants spent sufficient time in reading the materials and answering questions.

This study only recruited U.S. resident workers on MTurk. Inclusive criteria are people who have worked full time for at least six months and aged from 30-64 as they are the ones who are more likely to see and understand the implications of a data breach to their financial status. Full-time working people who are at least 30 years of age also have an earnings history and are more likely to rely on their credit score/reputation for purchases (e.g., housing mortgage, loan) than those who are in their 20s which may have a limited earnings history and are less likely to care about the risks associated with a data security breach.

G-power analysis was conducted to determine sample size. At given α=.05, power = 0.95, and effect size f = 0.25, a total sample size of 400 was required for this study. There were 446 subjects participated in an online experiment through Qualtrics, an online survey software. Each group had 33 to 35 participants. This online experiment was posted on MTurk to recruit sample participants with the titled "Data Breach 2." Each participant received $1 as a reward for taking part in the survey (the main study). There were 38 incomplete responses and one response was not acceptable, specifically the participant answered to work full-time for 25 years but claimed to be from 30-34 year-old. Although, the participant might mistakenly choose the wrong option, researcher argued that he or she might not pay attention to the study. Therefore, theses 39 responses were deleted. Four hundred and seven responses were valid and used for further analysis. Among 407 participants, participants who worked full-time for 4-10 years accounted for the highest percentage of survey-takers at 36.4 percent (N=148), followed by those who worked from 11-15 and 15-20 years at 16.2 percent (N=66) and 15.2 percent (N = 62), respectively. Participants who have more than 20 years accounted for 12.3 percent (N=50), followed by those who have 20-25 years at 12.3 percent (N = 50) and less than three years at 11.5 percent (N = 46). Participants' age ranged from 30 to 64 years. Participants who are in their 30s accounted for the highest percentage of 72.2 percent (N = 94). There were 211 (51.84%) male and 196 (48.16%) female participated in this study. The numbers of male and female participants were controlled to have a roughly equal representation of both gender. Except for four participants who chose not to reveal their highest education level, the percentages of participants who completed undergraduate, some post graduate or post-graduate degrees were 79.6 percent (N = 324), and those who have some high school or less, completed high school, some college or completed 2-year college were 19.4% (N = 79). The average number of people in the household was 3.12.

Table 1 shows demographic statistics including age, race, education, industry, total annual household income, number of debit and credit cards, relationship status, and number of people in the household.

Table 1. *Sample characteristics*

Variables	N	Percent (%)
Age		
30-34	206	50.6
35-39	88	21.6
40-40	41	11.1
45-49	25	6.1
50-55	16	3.9
55-59	19	4.7
60-64	12	2.9
Races		
African	68	16.7
Asian	47	11.5
Caucasian	121	29.7
Hispanic/Latino	125	30.7
Native American/Alaskan	34	8.4
Native Hawaiian/Pacific Islander	5	1.2
Two or more races	7	1.7

Highest education level		
High school graduate	14	3.4
Some college	43	10.6
2-year college graduate	22	5.4
4-year college graduate	184	45.2
Some post-graduate	29	7.1
Post-graduate degree	111	27.3
Prefer not to answer	4	1.0
Industry sector of employment		
Advertising	4	1.0
Communications	22	5.4
Construction	17	4.2
Education	51	12.5
Finance	78	19.2
Health care	44	10.8
Insurance	5	1.2
Investment	4	1.0
Manufacturing	38	9.3
Market research	18	4.4
Real estate	4	1.0
Retail	12	2.9
Sales	28	6.9
Technology	50	12.3

Others	32	7.9
Total annual household income		
Under $35,000	40	9.8
$35,000 - $49,999	71	17.4
$50,000 – 74,999	144	35.4
$75,000 - $99,999	83	20.4
$100,000 - $149,999	49	12.0
$150,000 - $199,999	6	1.5
$200,000 or more	7	1.7
Prefer not to answer	7	1.7
Number of debits and credit cards		
None	11	2.7
1	107	26.3
2	154	37.8
3	75	18.4
4 or more	60	14.7
Relationship status		
Single/never married	136	33.4
Married or domestic partner	244	60.0
Widowed	7	1.7
Divorced	17	4.2
Separated	3	0.7

Preliminary Test

This study conducted two preliminary tests to check the manipulation of independent variables. Two groups of students were used to test the message manipulation. One group of students exposed to the three messages of an external/uncontrollable causal attribution, explicit responsibility acceptance, and low sympathetic expression. The other student group exposed to the other three messages of an internal/controllable causal attribution, implicit responsibility acceptance, and high sympathetic expression. In the first pretest, thirty participants were randomly assigned to each condition. Results from the first pretest study indicated that there was no significant difference in the means between the group exposed to the external/uncontrollable causal attribution and the one exposed to the internal/controllable causal attribution. It was challenging for participants to determine who was primarily responsible for the crisis. Seven out of 30 participants made a note that they attributed a certain level of crisis responsibility toward the organization for failing to protect customers' personally identifiable information, regardless the cause(s) of the crisis. Thus, researcher added a self-defensive message to the external/uncontrollable causal attribution condition ("We, TechBuy, invest $10 million every year to strengthen our cybersecurity system to keep our customers' information secure") in order to be more controlled to the manipulation of the causal attribution message. After making this change in the statement, researcher conducted the second pretest with the participation of another thirty student participants. The same procedures were conducted. The statistical test of the second pretest was reported as follows.

Thirty participants were randomly assigned to each condition. There were 16 (53.33%) male and 14 (46.67%) female participants in this study. The average age of participants were 20 years old. Eight participants were juniors and 22 participants were sophomores.

To check the manipulation of causal attribution, this study assessed its two constructs, including the locus of responsibility and controllability. All items used a 7-point Likert-type scale ranging from 1(strongly disagree) to 7 (strongly agree). The measurement of the locus of responsibility, was adapted from Griffin, Babin, and Darden (1992) and Chung and Lee (2018), included three-item scale for blame, reporting an acceptable reliability (α = .87). The pretest primarily used a two-item scale for blame: *(1) Hackers, not TechBuy, are responsible for the crisis, and (2) The blame for the crisis lies in the hackers, not TechBuy.* An independent t-test for locus of control was conducted. The higher the value, the more likely a participant perceived that an external factor caused the crisis. Whereas, the lower the value, the more likely a participant perceived that an internal factor caused the crisis. The mean score was higher in the external/uncontrollable condition (*M* = 4.57, *SD* = 1.75) than the one in the internal/controllable condition (*M* = 3.03, *SD* = 1.37). There was a significant difference in the means (*t*(28) = 2.70, *p* = .012).

The measurement of controllability was adapted from the assessment of organizational control in Coombs and Holladay's (2002) study. Organizational control refers to the extent to which the organization can control a situation/event (Coombs & Holladay, 2002), reporting Cronbach's alphas reliability check ranging from .73 to .89. A three-items scale for organizational control was used in this pretest: *(1) The cause of the crisis is something TechBuy could control, (2) The cause of the crisis is something that was manageable by TechBuy, and (3) The cause of the crisis is something over which TechBuy had power*. An independent t-test for locus of control was conducted. The higher the value, the more likely a participant perceived a controllable crisis. Whereas, the lower the value, the more likely a participant perceived an uncontrollable crisis. The mean score for the manipulation check was higher in the controllable condition (*M* = 5.33, *SD* = 1.23) than the one in the uncontrollable condition (*M* = 4.19, *SD* = 1.32). There was a significant difference in the means (*t*(28) = -2.46, *p* = .021).

To check the manipulation of responsibility acceptance, participants were asked to rate how clearly the apology statement showed that TechBuy took responsibility for the data breach crisis. Participants were asked to choose either option 1 (implied) or option 2 (clearly stated). In the apology statement with implicit responsibility acceptance, 11 participants chose option 1 (implied) and three participants chose option 2 (clearly stated). In contrast, in the apology statement with explicit responsibility acceptance, six participants chose option 1 and 10 participants chose option 2. The index produced acceptable reliability ($\chi 2$(1)= 5.13, *p* = .033).

To check the manipulation of sympathetic expression, participants were asked to rate how well the apology statement showed that TechBuy highly expressed sympathy toward victims. Participants were asked to choose from either option 1 (very well) or option 2 (not very well). In the apology statement with high sympathetic expression, eight participants chose option 1 and six participants chose option 2. In contrast, in the apology statement with low sympathetic expression, three participants chose option 1 and 13 participants chose option 2. The index produced marginally acceptable reliability ($\chi 2$(1) = 4.74, *p* = .057). The p-value was in the borderline. Since the pretest was conducted with small sample (*N* = 30), it can be concluded that the index was reliable. However, Chi-square test is very low power. The sample size for the second pretest was small (n=30). Therefore, manipulation check was also conducted in the main study. The 7-point Likert-type scale used for checking the manipulation of causal attribution in the pretest was the same in the main study. However, the manipulation check for responsibility acceptance and sympathetic expression in the main study used a 7-point Likert-type scale (see Manipulation Check section in Chapter 4).

Measures of Dependent Variables

Anger relief. The five self-appraisal items for anger were adapted from Thomas and Millar (2008), McDonald et al. (2010), and Chung (2010). Chung's study (2010) reported a Cronbach's alpha at .94 after reading the news article and .96 after reading one of apology statements. The scale uses a 7-point Likert-type scale (*1 = not at all* and *7 = very much*) to measure the extent to which they agree with items. The five items were: (1) angry, (2) mad, (3) irritated, (4) annoyed, and (5) outraged. After reading a news articles, participants were asked to answer a question for each item, "To what extent do you feel […] (i.e., angry) toward the organization." Then, participants were asked to read an apology statement from TechBuy and answer these five questions again. The anger level was measured twice (after reading the news article and apology statement, respectively) by averaging the scores of these five items. The D-score of two average anger levels was calculated to measure the degree of anger relief, by subtracting the average anger value after reading the news article from the average anger value after reading the statement from TechBuy. A positive D-score means that anger was reduced to a certain level, while a negative one reflects the anger increased. A zero D-score equals to no anger relief. In this study, the index produced acceptable reliability at the value of Cronbach's alpha α = .94 and α = .93 after reading the news article and apology statement, respectively.

Organizational reputation. Measurements of corporate reputation were adapted from the three-item scale for corporate reputation by Weiss et al. (1999). The three-item scale uses a 7-point Likert-type scale (*1 = strongly disagree* and *7 = strongly agree*) to measure the extent to which they agree with items. The items were: *(1) TechBuy is a highly-regarded company, (2) TechBuy is a successful company, and (3) TechBuy is a well-established company.* The index produced acceptable reliability (α = .87).

Degree of trust in organization's competence. The five-item scale for competence was adapted from Mayer and David's study (1999) that reported Cronbach's alphas at .85 and .88. The scale uses a 7-point Likert-type scale (*1 = strongly disagree* and *7 = strongly agree*) to measure the extent to which they agree with items. The items were: *(1) TechBuy seems to be capable of protecting consumer's identity, (2) TechBuy seems to be known to be successful at protecting consumers' identity, (3) TechBuy seems to have much knowledge about handling data breaches, (4) TechBuy seems to have skills in protecting consumers' identity, (5) TechBuy seems to have specialized capacities to protect consumers' identity, and (6) TechBuy seems to be qualified in handling its data breach.* The index produced acceptable reliability (α = .96).

Degree of trust in organization's benevolence. The five-item scale for benevolence was adapted from Mayer and David's study (1999) that reported Cronbach's alphas at .87 and .89. The scale used a 7-point Likert-type scale (*1 = strongly disagree* and *7 = strongly agree*) to measure the extent to which they agree with items. The items were:*(1) TechBuy is very concerned with my welfare, (2) My needs and desires are very important to TechBuy, (3) TechBuy would not knowingly do anything to hurt me, (4) TechBuy really looks out for what is important to me, and (5) TechBuy will go out of its way to protect my identity from the data breach.* The index produced acceptable reliability (α = .92).

Degree of trust in organization's integrity. The six-item scale for integrity was adapted from Mayer and David's study (1999) that reported Cronbach's alphas at .82 and .83. The scale uses a 7-point Likert-type scale (1 = strongly disagree and 7 = strongly agree) to measure the extent to which they agree with items. The items were: *(1) TechBuy has a strong sense of justice, (2) I never have to wonder whether TechBuy will stick to their word, (3) TechBuy tries hard to be fair in dealing with its customers, (4) TechBuy's actions and behaviors are not very consistent* (reversely recoded), *(5) I like TechBuy's values, and (6) Sound principles seem to guide TechBuy's behavior.* The index produced acceptable reliability (α = .78).

Procedures

Participants on MTurk read an invitation message that describes the purpose of the study and eligible conditions to participate in the study. Only people who are at least 30 years old and have full-time employment at least six months in the United States were qualified to participate in the study. Participants clicked the link included in the invitation message that directed them to the online experiment on Qualtrics. If participants were eligible and agreed to the consent form, they were randomly assigned to one of 12 groups. First, participants will be asked to read a fictional news article about a data breach incident happened to TechBuy. The fictional news article was modified from the news article about the Target data breach in 2013 (McGrath, 2014). The fictional news article described the incident and the type of consumers' information that was compromised. After reading the news article, participants were asked to answer questions about their feeling of anger. Then, they continued to read one of 12 organizational statements. The news article was used to provide background information about TechBuy and its data breach incident. A one-way ANOVA was conducted after participants read the news article in order to test whether participants' level of anger in the 12 groups were significant. The results of this baseline anger relief analysis were reported in Chapter 4. In crisis communications practice, a statement (also called *notification)* is sent to affected customers when a data breach incident occurs. In this experimental study, participants were asked to assume that they were affected customers of the data breach incident when they read one of the twelve statements assumingly being sent by TechBuy. Each statement was a combination of causal attribution (internal vs. external), responsibility acceptance (none, implicit, explicit), expression of sympathy toward victims (high vs. low). After reading the apology statements, participants were asked to answer questions about their feelings of anger again in order to measure the level of anger relief, perceptions of organizational reputation, and the degree of trust in the organization's competence, integrity, and benevolence. It took each participant approximately 15 to 25 minutes to complete the survey. The questionnaires also asked demographic information, including participants' employment status, number of years of full-time employment, age, gender, ethnicity, education, industry they are working in, and annual household income before taxes, number of debit and credit cards, relationship status, and number of people in the household.

Data Analysis

To test the main effect of causal attribution (hypothesis 1a and 1b) and sympathetic expression (hypothesis 3), t-tests were conducted. A one-way analysis of variance (ANOVA) was performed to test the main effect of responsibility acceptance (hypothesis 2). To determine how to analyze interaction effects of the three independent variables (H4a, H4b, H4c, and H5), researcher first ran a Pearson correlation coefficient for anger relief (D-score), reputation, and trust in competence, benevolence, and integrity. Results from this test were analyzed in order to determine how to test the interactions among dependent variables. Weak correlations, that were not significant, were found between anger relief and reputation ($r(405) = -.08, p = .105$), trust in competence ($r(405) = -.07, p = .143$) and benevolence ($r(405) = -.08, p = .09$). However, anger relief was significantly correlated with trust in integrity ($r(405) = -.14, p < .05$). Thus, a three-way ANOVA was conducted to test the interactions between and among independent variables on public anger relief. Reputation were moderately correlated to trust in competence ($r(405) = .43, p < .01$), benevolence ($r(405) = .46, p < .01$), and integrity ($r(405) = .47, p < .01$). Since trust in competence, benevolence, and integrity are three components of trustworthiness which is central in understanding and predicting trust levels (Colquitt et al., 2007), these three variables were significantly correlated. Correlations between trust in competence and benevolence were ($r(405) = .81$, $p < .01$) and between competence and integrity were ($r(405) = .76$, $p < .01$). Although dependent variables correlated from about .3 to .7 were recommended to be eligible for using a MANOVA (Maxwell, 2001), researcher argues that the correlations between reputation and three trust factors were not too high. Therefore, it is acceptance for using a three-way multivariate analysis of variance (MANOVA) to test the interactions between and among independent variables on public anger relief on reputation and trust in organization's competence, benevolence, and integrity.

Chapter 4: Results

Manipulation Check

To check whether the manipulations of independent variables were effective, independent t-tests for causal attribution by apology statements were conducted. The main study asked the same questions for locus of control and controllability used in the pretest. For the locus of control, the mean for the manipulation check was higher in the external condition (*M* = 4.89, *SD* = 1.42) than in the internal condition (*M* = 4.23, *SD* = 1.54). There was a significant difference in the means (*t*(405) = 4.40, *p* < .01). For controllability, the mean score for the manipulation check was higher in the controllable condition (*M* = 5.33, *SD* = 1.15) than the one in the uncontrollable condition (*M* = 5.09, *SD* = 1.26). There was a significant difference in the means (*t*(28) = -2.05, *p* < .05).

In the main study, the 7-point scales to check the manipulations of responsibility acceptance and sympathetic expressions were used. Participants were asked to rate the extent to which they agreed with the statement in a 7-point scale ranging from 1 (strongly disagree) to 7 (strongly agree). For the responsibility acceptance, a three-item scale was used: *(1) The apology from TechBuy explicitly took responsibility for the crisis, (2) The apology from TechBuy implicitly took responsibility for the crisis, and (3) The apology from TechBuy explicitly did not take responsibility for the crisis*. For the responsibility acceptance, the item was: *The apology from TechBuy highly expressed sympathy toward the victims.* An independent t-test for sympathetic expression by apology statements was conducted. The main study asked participants to rate the extent to which they feel TechBuy highly expressed sympathy toward victims. The mean for the manipulation check was higher in the high sympathy condition (*M* = 4.97, *SD* =

1.57) than in the low sympathy condition (*M* = 4.28, *SD* = 1.79). There was a significant difference in the means (*t*(405) = 4.13, *p* < .01).

A one-way ANOVA was conducted to check the manipulation of responsibility acceptance. There was a significant difference in the means of the three levels of responsibility acceptance (*F*(2, 404) = 3.27, *p* < .05). Tukey HSD test indicated that the mean score for explicit responsibility acceptance (*M* = 4.85, *SD* = .97) was significantly different from the implicit responsibility acceptance (*M* = 4.52, *SD* = 1.04). However, neither the mean score of explicit responsibility acceptance nor implicit responsibility acceptance significantly differed from the mean score of the no statement of responsibility acceptance (*M* = 4.66, *SD* = 1.12).

Baseline anger

Hypothesis testing of independent variables on anger relief used the D-value that was the subtraction of the average anger score after reading the news articles and the average score after reading the one of the 12 statements.

However, baseline anger, which was the average anger score after reading the news articles, was also analyzed to examine the level of anger after reading the news article. A one-way ANOVA was conducted to compare the means of anger levels between the 12 groups after reading the news article to examine whether participants' anger level was the same or similar in different groups after reading the news article. The ANOVA result indicated that there was no significant difference on anger level between the 12 groups after reading the news article (*F*(11, 395) = 1.06, *p* = .39).

Hypotheses testing

Main effects of causal attribution. Hypothesis 1a stated that participants who read an apology statement with an external/uncontrollable causal attribution are more likely to (a) reduce anger, (b) hold a positive perception on organizational reputation, and (c) have higher trust in an organization's competence, (d) benevolence than those who read an apology statement with an internal/controllable causal attribution. Hypothesis 1b stated that there is no significant difference in participants' trust in an organization's integrity between those who read an apology statement with an external/uncontrollable causal attribution and those who read the one with an internal/controllable causal attribution.

To test hypotheses 1a and 1b, an independent t-test was used to compare the dependent variables' mean score of participants who read the apology statement with external/uncontrollable causal attribution to those of who read the apology statement with internal/controllable causal attribution. Results outlined in Table 2 indicated that there were significant differences between internal/controllable causal attribution group (n = 203) and external/uncontrollable causal attribution group (n = 204) on anger relief ($t(405) = -2.18$, $p < .05$), trust in an organization's competence ($t(405) = 3.02$, $p < .01$), and benevolence (($t(405) = 2.21$, $p < .05$). The mean score for external/uncontrollable causal attribution ($M = -.22$, $SD = .98$) was higher than the mean score for the internal/controllable causal attribution ($M = .01$, $SD = 1.15$) on individuals' anger relief. The mean score for external/uncontrollable causal attribution ($M = 4.40$, $SD = 1.62$) was also higher than the mean score for the internal/controllable causal attribution ($M = 3.91$, $SD = 1.62$) on individuals' trust in organization's competence. Similarly, the mean score for external/uncontrollable causal attribution ($M = 4.64$, $SD = 1.43$) was significantly different from the internal/controllable causal attribution ($M = 4.33$, $SD = 1.43$) on individuals' trust in organization's benevolence. However, there was no significant difference between two groups of causal attributions on organizational reputation ((*t*(405) = 1.49, *p* = .137). The mean score for external/uncontrollable causal attribution (*M* = 5.46, *SD* = 1.15) was not significantly different from the internal/controllable causal attribution (*M* = 5.29, *SD* = 1.18) on individuals' perception of organizational reputation. Hypothesis 1a (a), (c), (d) were supported.

There was no significant difference between two groups of causal attributions on trust in an organization's integrity ((*t*(405) = 1.55, *p* = .122). The mean score for external/uncontrollable causal attribution (*M* = 4.36, *SD* = 1.12) was not significantly different from the internal/controllable causal attribution (*M* = 4.21, *SD* = 1.10) on individuals' trust in organization's integrity. Cohen (1988) classified the values of *d* of 0.2, 0.5, or 0.8 as "small," "medium," and "large" effect sizes, respectively. The effect sizes in this test ranged from 1.13 to 0.30, suggesting that the effect sizes were small. Hypothesis 1b was supported.

Table 2. *Results of t-test and descriptive statistics for causal attribution*

	Causal attribution							
	External/ uncontrollable		Internal/ Controllable					
Dependent variables	M	SD	M	SD	*95% CI for mean difference*	*t*	*d*	*p*
Anger relief	-.22	0.98	.01	1.12	-.43, -.02	-2.18	.22	.030
Reputation	5.46	1.15	5.29	1.18	-.06, .40	1.49	.15	.137
Trust in competence	4.40	1.62	3.91	1.62	.17, .80	3.02	.30	.003
Trust in benevolence	4.64	1.43	4.33	1.43	.03, .59	2.21	.22	.028

Trust in integrity	4.36	1.12	4.21	1.11	-.07, .37	1.37	.13	.171

Main effects of sympathetic expression. Hypothesis 2 stated that participants who read an apology statement with an explicit responsibility acceptance is more likely to (a) reduce anger, (b) hold a positive perception on organizational reputation, and (c) have higher trust in an organization's competence, benevolence than those who read an apology statement with an implicit responsibility acceptance.

A one-way ANNOVA was used to compare the mean scores of participants' responses who read the apology statement with one of three different levels (explicit, implicit, and none) of responsibility acceptance. Results outlined in Table 3 indicated that a significant difference was found among participants' responses at three different levels of responsibility acceptance on organizational reputation ($F(2,404)=3.45$, $p < .05$), and trust in organization's competence ($F(2,404)=4.19$, $p < .05$), benevolence ($F(2,404)=6.50$, $p < .05$), and integrity ($F(2,404)=5.39$, $p < .01$). There was no statistically significant difference among the three levels of responsibility acceptance on participants' perception on anger relief ($F(2,404)= .06$, $p = .944$). Although results from the one-way ANOVA showed the overall differences (if any) between groups, they did not tell which specific groups differed.

Tukey HSD test, also known as post hoc test, was used to identify which groups differed. Results indicated that the mean score for explicit responsibility acceptance ($M = 5.56$, $SD = 0.97$) was higher than the mean score for the implicit responsibility acceptance ($M = 5.12$, $SD = 1.14$) on individuals' perception of organizational reputation. However, neither explicit responsibility acceptance nor implicit responsibility acceptance significantly differed from the no statement of responsibility acceptance ($M = 5.38$, $SD = 1.25$) on individuals' perceptions of organizational reputation. The mean scores at different levels of responsibility acceptance were much higher than the mid-point of the 7-Likert scale. It indicated that an explicit responsibility acceptance could contribute significantly to generate favorable perception on reputation.

The mean score for explicit responsibility acceptance (*M* = 4.81, *SD* = 1.30) was higher than the mean score for the implicit responsibility acceptance (*M* = 4.19, *SD* = 1.56) on individuals' trust in organization's benevolence. However, neither explicit responsibility acceptance nor implicit responsibility acceptance was significantly difference from the no statement of responsibility acceptance (*M* = 4.46, *SD* = 1.39) on individuals' trust in organization's benevolence.

Similarly, the mean score for explicit responsibility acceptance (*M* = 4.51, *SD* = .95) was higher than the mean score for the implicit responsibility acceptance (*M* = 4.07, *SD* = 1.20) on individuals' trust in integrity. However, neither explicit responsibility acceptance nor implicit responsibility acceptance was significantly difference from the no statement of responsibility acceptance (*M* = 4.27, *SD* = 1.11) on individuals' trust in integrity.

The mean score for implicit responsibility acceptance (*M* = 3.82, *SD* = 1.73) was significantly different from the explicit responsibility acceptance (*M* = 4.32, *SD* = 1.58) and no statement of responsibility acceptance (*M* = 4.32, *SD* = 1.56) on individuals' trust in organization's competence. However, the explicit responsibility acceptance did not significantly differ from the no statement of responsibility acceptance on individuals' trust in organization's competence.

The mean score for explicit responsibility acceptance (*M* = -0.08, *SD* = 1.09) was not significantly different from the implicit responsibility acceptance (*M* = -0.10, *SD* = 1.0) or the no statement of responsibility acceptance (*M* = -0.12, *SD* = 1.08) on individuals' anger relief.

Taken together, these results suggest that explicit responsibility acceptance do have effect on individual's perception of organizational reputation, trust in organization's competence, benevolence, and integrity. However, it is noted that explicit responsibility acceptance should be stated with a statement with an acceptance of full responsibility. The implicit responsibility acceptance does not appear to significantly generate favorable perception of reputation and trust in the organization. Hypothesis 2(b), (c), (d), and (e) were supported.

Table 3. *Results of a one-way ANOVA for responsibility acceptance*

	Responsibility acceptance								
Dependent	Explicit		Implicit		None				
variables	M	SD	M	SD	M	SD	*F*	η^2	*p*
Anger relief	-.08	1.09	-.10	1.0	-.12	1.08	.06	-.01	.944
Reputation	5.56	0.97	5.19	1.24	5.38	1.25	3.45	.02	.033
Trust in competence	4.32	1.58	3.82	1.73	4.32	1.56	4.12	.06	.016
Trust in benevolence	4.81	1.30	4.19	1.56	4.46	1.39	6.50	.08	.002
Trust in integrity	4.51	.95	4.07	1.20	4.27	1.14	5.39	.04	.005

Main effect sympathetic expression. Hypothesis 3 stated that participants who read an apology statement with high sympathetic expression have no different reactions in terms of (a) relieving anger, (b) perceiving organizational reputation, and (c) trusting in an organization's competence, benevolence than those who read an apology statement with low sympathetic expression.

An independent t-test was used to compare the mean score of participants who read the apology statement with high sympathetic expression to the mean score of those read the apology statement with low sympathetic expression. Results outlined in Table 4 indicated that there were no statistically significant differences between high sympathetic expression group (n = 204) and low sympathetic expression group (n = 203) on anger relief (*t*(405) = -1.58, *p* = .115), organizational reputation (*t*(405) = -.70, *p* = .488), trust in an organization's competence (*t*(405) = .575, *p* = .565), and benevolence (*t*(405) = 1.60, *p* = .110) and trust in organization's integrity (*t*(405) = 1.75, *p* = .081).

The mean score for high sympathetic expression group (*M* = -.19, *SD* = 1.05) was not significantly different from low sympathetic expression group (*M* = -.02, *SD* = 1.05) on individuals' anger relief. The mean score for high sympathetic expression group (*M* = 5.33, *SD* = 1.12) was not significantly different from low sympathetic expression group (*M* = 5.42, *SD* = 1.14) on individuals' perceptions on organizational reputation. The mean score for high sympathetic expression group (*M* = 4.20, *SD* = 1.63) was not significantly different from low sympathetic expression group (*M* = 4.11, *SD* = 1.65) on individuals' trust in organization's competence. The mean score for high sympathetic expression group (*M* = 4.60, *SD* = 1.45) was not significantly different from low sympathetic expression group (*M* = 4.37, *SD* = 1.43) on individuals' trust in organization's benevolence. Similarly, the mean score for high sympathetic expression group (*M* = 4.38, *SD* = 1.10) was not significantly different from low sympathetic expression group (*M* = 4.19, *SD* = 1.12) on individuals' trust in organization's integrity. The effect sizes in this test ranged from 0.05 to 0.17, suggesting that the effect size were small. Hypothesis 3 was supported.

Table 4. *Results of t-test and descriptive statistics for sympathetic expression*

Dependent variables	Sympathetic expression				*95% CI for mean difference*	*t*	*d*	*p*
	High		Low					
	M	SD	M	SD				
Anger relief	-.19	1.05	-.02	1.05	-.37, -.04	-1.58	.16	.115
Reputation	5.33	1.12	5.42	1.14	-.31, .15	-.70	.08	.488
Trust in competence	4.20	1.63	4.11	1.65	.23, .41	.58	.05	.565
Trust in benevolence	4.60	1.45	4.37	1.43	0.05, 0.51	1.60	.16	.110
Trust in integrity	4.38	1.10	4.19	1.12	-0.02, 0.41	1.75	.17	.081

Interaction of causal attribution, responsibility acceptance, and sympathetic expression. A three-way ANOVA and three-way MANOVA were used to test hypotheses 4a, 4b, 4c, and 5. The three-way ANOVA tested the interaction effects of independent variables on anger relief, while the three-way MANOVA tested the interactions of independent variables on other dependent variables.

Hypotheses 4a and 4b predicted the interaction effects of causal attribution and responsibility acceptance. Hypothesis 4a stated that under an internal/controllable crisis situation, participants who read an explicit responsibility acceptance are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust the organization’s (c) competence, (d) integrity, and (e) benevolence than those who read an implicit responsibility acceptance. Hypothesis 4b stated that under an internal/controllable crisis situation, participants who read an implicit responsibility acceptance are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust the organization's (c) competence, (d) integrity, and (e) benevolence than those who read an apology without a responsibility acceptance. The three-way ANOVA results also showed the results from the comparison of the mean scores for participants who read one of three statements with different levels of responsibility acceptance and who read the statement revealing either external/uncontrollable or internal/controllable causal attribution. The interaction was not significant (*F*(2,401) = 1.99, *p* = .139). Thus, it indicated that the interaction of responsibility acceptance and causal attribution has no significant effect on anger relief. The mean score for internal/controllable and explicit responsibility acceptance group (*M* = .08, *SD* = .94) was not significantly different from internal/controllable and implicit responsibility acceptance group (*M* = -.13, *SD* = 1.16) on individuals' anger relief. Moreover, the three-way MANOVA results showed that none of other dependent variables were significantly influenced by the interaction of causal attribution and responsibility acceptance (λ (8, 784) = .967, *p* = .110). Hypotheses 4(a) and 4(b) were not supported.

Hypotheses 4c predicted that the interaction effects of responsibility acceptance and sympathetic expression. Hypothesis 4c stated that under an internal/controllable crisis situation, participants who read a high sympathy expression are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust the organization's (c) integrity and (d) benevolence than those who read a low sympathy expression. The three-way ANOVA results also showed the results from the comparison of the mean scores for participants who read one of three statements with different levels of responsibility acceptance and who read the statement with either high or low sympathetic expression. The interaction was not significant (*F*(2,401) = .232, *p* = .793). Thus, it indicated that the interaction of responsibility acceptance and sympathetic expression has no significant effect on anger relief. The mean score for internal/controllable and high sympathetic expression group (*M* = -.13, *SD* = 1.26) was not significantly different from internal/controllable and implicit responsibility acceptance group (*M* = .03, *SD* = 1.04) on individuals' anger relief. Moreover, the three-way MANOVA results showed that no significant interaction effect between the responsibility acceptance and sympathetic expression was found on other dependent variables (λ (8, 784) = .963, *p* = .064). Hypotheses 4(c) was not supported.

Hypotheses 5 predicted that the interaction effects of causal attribution, responsibility acceptance, and sympathetic expression. Hypothesis 5 stated that under an internal/controllable crisis situation, participants who read an explicit responsibility acceptance and high sympathy expression are more likely to (a) reduce anger, (b) hold a positive organizational reputation, and trust in organization's (c) competence, (d) integrity, and (e) benevolence than those who read an implicit responsibility acceptance and low sympathetic expression. The three-way ANOVA results also showed the results from the comparison of the mean scores for participants who read one of three statements with different levels of responsibility acceptance and who read the statement with either high or low sympathetic expression at either external/uncontrollable or internal/controllable causal attribution. The interaction was marginally significant (*F*(2,401) = .292, *p* = .055). Thus, it indicated that the interaction of causal attribution, responsibility acceptance, and sympathetic expression has marginal significant effect on anger relief. Under internal/controllable causal attribution, the mean score of explicit responsibility acceptance and high sympathetic expression group (*M* = -.40, *SD* = 1.41) was marginally significantly different from the mean score of implicit responsibility acceptance and low sympathetic expression one (*M* = -.14, *SD* = 1.0) on individuals' anger relief. Moreover, the three-way MANOVA results showed that the interaction of causal attribution, responsibility acceptance, and sympathetic expression was statistically significant (λ(8, 784) = .958, p = .03). However, follow-up univariate ANOVAs indicated that the scores were not statistically significant for reputation (F(2,395) = .773, p = .462), trust in competence (F(2,395) = .024, p = .976), trust in benevolence (F(2,395) = .123, p = .885), and trust in integrity (F(2,395) = 1.46, p = .233). The interactions of causal attribution, responsibility acceptance, and sympathetic expression have no significant effects on organizational reputation and trust in competence, benevolence, and integrity. Thus, only hypothesis 5(a) was marginally supported.

To sum up, the main effects of causal attribution (H1a (a), (c), and (d)) on anger relief, and trust in an organization' competence and benevolence were supported. The main effects of responsibility acceptance (H2b, c, d, e) on perception of organizational reputation, and trust in an organization's competence, benevolence, and integrity were supported. Under the internal/controllable causal attribution, the interactions of responsibility acceptance and sympathetic expression (5a) has a marginal significant effect on reducing public anger. The null hypotheses, including the effects of causal attribution on trust in an organization's integrity (H1b) and the main effects of sympathetic expression (H3), were supported, with an acknowledgement of the limitations of these findings. The next chapter discussed findings, limitations and future research, theoretical and practical implications, and concluded the study.

Chapter 5: Discussion

This study examined the effects of causal attribution and apology's components, specifically responsibility acceptance and sympathetic expression, on stakeholder responses, including anger relief, organizational reputation, and trust in the organization's competence, integrity, and benevolence. Causal attribution is viewed as one of the basic tenets of Situational Crisis Communication Theory (SCCT) (Coombs & Holladay, 1997). It is suggested that causal attribution reflects how stakeholders determine the extent to which they attribute crisis responsibility toward an organization, which in turn could affect their reactions toward an organization (Coombs & Holladay, 2002). This study found that individuals are more likely to reduce anger when they perceived a crisis to be caused by an external/uncontrollable factor than the one caused by an internal/controllable factor. This finding is consistent with Weiner's argument (1985) that people tend to be sympathetic to the organization involved in a crisis that is uncontrollable or caused by external factor(s). This finding is also consistent with prior SCCT-based research (e.g., Boston et al., 2007; Darley & Pittman, 2003) indicating that apologies for a transgression due to external/uncontrollable factors could help to reduce stakeholders' anger. A possible explanation is that individuals tend to accept apologies and forgive a transgression that was made unintentionally. Thus, providing information regarding the nature of a crisis could help individuals to make informed decision whether an organization is a victim of a crisis. It also shows that the organization can identify the cause of the crisis, which may indicate that the organization has the ability to handle the situation (trust in competence). Knowing the organization's ability of fixing an issue can reduce the induced anger and encourage individuals to have interactions with the organization (trust in benevolence). Findings in this study confirmed that participants are more likely to trust the organization's competence and benevolence when they perceived a crisis is caused by external/uncontrollable factor.

Image restoration theory (IRT) and situational crisis communication theory (SCCT) served as theoretical frameworks in this study. IRT suggests that maintaining a favorable reputation is a key goal of crisis communications. Mortification strategy, in which the accused accepts responsibility and asks for forgiveness, is recommended to restore organizational image (Benoit, 1995). Apology strategy in SCCT suggests the organization to take full responsibility for the crisis and ask stakeholders for forgiveness in order to reduce the amount of reputational damage caused by the crisis (Coombs, 2007). IRT and SCCT shared the idea that an apology should include an explicit statement of accepting responsibility when an organization's reputation is threatened in a crisis (Benoit, 1995; Coombs & Holladay, 2008; Lazare, 2004). Existing studies found that an explicit responsibility acceptance could help to reduce public anger (i.e., Lee, 2005; Pace et al., 2012). Understanding what components of an apology could reduce individuals' anger is crucial in crisis communications.

Findings in this study are consistent with prior SCCT studies regarding the relationship between an organization's responsibility acceptance and positive public perceptions toward the organizational reputation (i.e., Claeys et al., 2010; Pace et al., 2012). Specifically, an apology with an explicit responsibility acceptance to a transgression-based crisis could gain positive stakeholders' views of organizational reputation (Pace et al., 2012). If a data breach crisis really occurs (the organization confirmed the incident), then it is recommended that the company apologizes and accepts responsibility in crisis responses to mitigate reputational damage. Stakeholders judge crisis responsibility based on information they receive, including mediated reports or organization's statement (Coombs, 2007). Weiner, Graham, Peter, and Zmuidinas

(1991) found that accepting responsibility could increase forgiveness and sympathy toward the organization. Additionally, people tend to perceive organizational reputation negatively when they considered a crisis to be severe (Claeys et al., 2010; Coombs, 1998). Therefore, organizations should consider apologize and accept responsibility when the perceived crisis responsibility is severe.

Moreover, findings in this study are consistent with existing studies (e.g., Lewicki et al., 2016; Park, Lee, & Kim, 2013), showing that an explicit statement of responsibility acceptance could rebuild trust in all aspects of competence, benevolence, and integrity. Keh and Xue argued that trust and reputation are correlated. If an explicit apology contributes to favorable perceptions of organizational reputation, it rebuilds trust in an organization. In a data breach incident, people tend to question the organization's competence in protecting their customers' personally identifiable information. In other words, a data breach is considered as a trust-based transgression. Moreover, an explicit apology also indicates that the organization's willingness to fulfill ethical and legal obligations (integrity), thereby, could induce emotional and affective bonds with its stakeholders (benevolence).

Using sympathetic expression is recommended when the perceived crisis responsibility is mild (Bennett & Earwalker, 2001). The challenge is how to express sympathy in a way that the sympathizer and sufferer shared similar feelings. In other words, a sympathetic expression should help the sufferer knows that a person is sympathizing and the sympathizer really feels so. This study examined the different effects of high and low sympathetic expression. Since the fictional data breach scenario used in this study was designed as a severe incident, findings found that only expressing sympathy, either low or high level, would not contribute to gain favorable public responses. In other words, sympathetic expression should be used along with other crisis response strategies in order to gain favorable public reactions.

It is surprising that no interaction effect of responsibility acceptance and sympathetic expression was found on public responses. This finding was inconsistent with existing studies. Specifically, Patel and Reinsch (2003) found that apologies with sympathetic expression were more effective. Sympathetic expression, used along with highly accommodative strategies (i.e., apology strategy), focuses on sharing victims' feelings or suffering that could help to rebuild organization-public relationship (Coombs & Holladay, 2008; Diers-Lawson & Pang, 2016). Expressing sympathy makes apologies appear to be sincere (Weiner, 1985). Findings in this study indicated that individuals might expect to know about detailed corrective actions in addition to a statement of responsibility acceptance and sympathetic expression. It is also due to the nature of an experimental study in which study participants were not the real victims of a fictional crisis incident. Future studies could recruit individuals who were affected customers in a real data breach incident.

The interaction effect of causal attribution, responsibility acceptance, and sympathetic expression was only found on anger relief. Specifically, under external/uncontrollable causal attribution, a statement with explicit responsibility acceptance and high sympathetic expression reduce public anger compared with the one with implicit responsibility acceptance and low sympathetic expression. This study is consistent with the ideas outlined in SCCT in that indicates when crisis responses match the level of attributed crisis responsibility, crisis response outcomes tend to gain favorable public responses (Coombs, 1997; Coombs & Holladay, 2002). Thus, it is crucial to choose appropriate apologetic components in response to different causal attributions.

Theoretical Implications

One theoretical implication of this study is the examination of causal attribution's effects on public responses in data breach crises. Data breach is a unique crisis type in which, regardless of what causes the incident, stakeholders always attribute certain amount of crisis responsibility to the organization for failing to protect their personal information. Findings in the pretest study revealed that stakeholders attribute certain level of crisis responsibility toward the breached organization, regardless the cause(s) of the data breach incident. It is unlike other crisis types where, when stakeholders know the cause(s) of a crisis incident, they could determine either an organization or external factor(s) caused a crisis. This finding is in line with Bentley et al.'s argument that data breach crises have ambiguous causal attribution (2018), which is challenging for stakeholders to determine who is primarily responsible for the crisis. Moreover, findings in this study regarding the different effects of causal attribution on public anger relief and trust in an organization's competence and integrity has added evidence to the role of causal attribution in the determination of crisis responsibility, which is one of the key points in the situational crisis communication theory.

This study found that anger decreases when stakeholders understand the nature or cause(s) of a crisis incident. Although SCCT and IRT emphasized the importance of reducing reputational damage or repairing organizational image by choosing appropriate crisis responses, relieving individuals' anger toward an organization in time of crisis could contribute to a positive outcome of crisis responses. Since anger can be elicited during situation of physiological arousal (Lazarus, 1991), a high level of anger could motivate individuals to act on voicing their concerns (e.g., word-of-mouth, post or comments about the issue on social media), protesting or boycotting. Thus, relieving public anger is also a critical goal of crisis responses. Not many organizations are willing to reveal the cause(s) of a crisis incident, particularly when it was caused by an internal/controllable factor for fear of gaining more attention or critics or avoiding embarrassing the organization itself. However, providing information about the cause of a crisis incident indicates the organization's integrity or willingness to investigate and solve the issue. It also helps stakeholders determine crisis responsibility attribution, thereby, affecting their reactions to the organization.

Although under external/uncontrollable causal attribution, this study found marginally significant effect of explicit responsibility acceptance and high sympathetic expression compared with a statement with implicit responsibility acceptance and low sympathetic expression, this indicated that the interactions of different components in a statement did have certain impact on reducing public anger. This finding suggests that responding to a severe crisis requires rigorous apologies and the organization appearing to be transparent in their crisis responses in order for stakeholders to make informed decision on crisis responsibility attribution. When the crisis responses matched the level of crisis responsibility attribution, it could help to reduce public anger.

Another contribution of this study is the examination of the role of apologies in crisis responses and how to apologize appropriately. This study found that an explicit statement of responsibility acceptance could generate more favorable perceptions of organization's reputation. Using a full apology with explicit responsibility acceptance when an organization chooses to use apology strategy (as outlined in SCCT) or mortification strategies (as outlined in IRT) could increase the effectiveness of crisis response efforts. Moreover, although Coombs and Holladay (2008) found that apologies were no more effective at improving attitudes toward an organization than offering compensation or expressing sympathy, this study found that no significant effects of sympathetic expression in severe crises. In other words, sympathetic expression should be used along with other crisis communication messages (i.e., apologies, corrective actions in severe crises.

Finally, instead of examining trust as one dependent variable, this study used three elements of trustworthiness, which is a central in understanding and predicting trust levels (Colquitt et al., 2007), to examine stakeholder perception on their trust in organization's competence, benevolence, and integrity. Very few studies examined trust using the three elements of trustworthiness (Park et al., 2013). When trust was often measured as one variable, without considering detailed elements contributing to the formulation of trust (i.e., Bentley et al., 2018), it did not allow researchers to see changes in stakeholders' trust in various aspects of an organization. Regaining trust in the organization is an important outcome of crisis response efforts. This study found that an organization's statement that explicitly accepts responsibility of a crisis could gain trust in the organization in terms of competence, benevolence, and integrity. However, findings in this study indicated that revealing the nature or cause(s) could regain trust in organization's competence and benevolence. Specifically, stakeholders tend to trust an organization's competence, which indicates the organization's knowledge, skills, and experience in specific areas, when a crisis was caused by external/uncontrollable factor(s). Stakeholders were found to be more likely to sympathize to the organization when the crisis was caused by external/uncontrollable factor(s), which in turn, reinforce emotional and affective bonds as well as maintain or enhance interactions between stakeholders' and the organization (trust in benevolence). Thus, it is crucial to understand the effects of each component of an apology to rebuild trust in an organization's competence, benevolence, and integrity.

Practical Implications

It is an important to consider what components should be included in an organizational apology in response to a crisis. Understanding the effects of different apologetic components could help crisis managers determine how to structure crisis communication messages or a statement. Moreover, anger relief, reputation restoration, and rebuilding trust in an organization are among important outcomes of crisis response efforts. In severe crisis incident, crisis managers may want to consider using apology strategies. Findings in this study suggest that crisis managers should inform stakeholders about the nature of a crisis incident and consider the extent to which the organization should accept responsibility. Informing stakeholders about the cause of a crisis incident helps them understand the problem and determine crisis responsibility attribution. It also helps the organization appear to be transparent and shows willingness to investigate and fix the issue. Thereby, it could help to reduce stakeholders' anger and regain their trust in the organization's competence and benevolence.

An explicit responsibility acceptance should be used when a crisis incident is considered as severe in order to gain favorable perceptions of reputation and rebuild trust in an organization's competence, benevolence, and integrity. Under external/uncontrollable causal attribution, an apology with explicit responsibility acceptance and high sympathetic expression was found to reduce public anger compared with an apology with a simple apology and low sympathetic expression. It indicates that choosing appropriate words in an apology statement would help to reduce stakeholders' anger. Scholars suggested that the more apologetic components were used in an apology statement, the more likely crisis responses would be in gaining positive public reactions (Benoit, 1997; Lewicki et al., 2012). Thus, expressing sympathy and taking full responsibility in a transgression are recommended to gain positive public responses.

Limitations and Future Research

The current study has several limitations. First, the statement's messages may have oversimplified the nature of data breach crises. Since the study examined the effects of causal attribution, the statements were designed to reveal the cause of the fictional data breach crisis. However, revealing the nature of the data breach was optional in all data breach notification state laws. If the incident was caused by the organization by mistake, the organization tends to focus on highlighting their responding actions rather than embarrassing themselves by detailing the cause(s) of the incident. If the hackers purposely attack an organization's database, the organization tends to defend itself to have a strong database firewall but hackers just have one job to find (a) weak point(s) in the firewall. Moreover, results from the pretest study indicated that whether a data breach incident is caused intentionally or unintentionally, stakeholders will attribute crisis responsibility to the organization for failing to protect the information they shared with the organization. The only difference in stakeholders' judgment about different cause(s) of an incident is the extent to which stakeholders attribute crisis responsibility (high vs. low) to the organization. Data breach incidents may have ambiguous crisis responsibility if the organization does not reveal the cause(s). Future research should examine individual's perception on cybersecurity risks associated with data breach incidents.

The design of news article and messages also have several limitations. The news article used in this study was not strictly followed the format of a news article. Additionally, the explicit responsibility acceptance message was limited for having a compound for not only taking responsibility acceptance but also claiming to "fix the problem", which implied to conduct correction actions. Thus, future research should test the effects of explicit responsibility acceptance with a full responsibility acceptance only.

Second, findings in this study indicated that a simple apology or a statement with an implicit responsibility acceptance may not sufficient to reduce public anger and gain favorable responses. This study results found a significant difference between an apology with an explicit responsibility acceptance and implicit responsibility acceptance. However, the nature of data breach scenario could affect stakeholders' perceptions. Future research should examine the effect of responsibility acceptance by comparing two crisis scenarios, including a data breach incident and another crisis type that stakeholders could determine only one entity (e.g., an individual, organization) responsible for the crisis.

Third, severe crises that significantly affect a large number of individuals (e.g., data breach incident) should include information regarding corrective actions in crisis communication messages. Crisis management aims to protect the public from any potential risks as well as reduce an organization's reputation damage (Coombs, 2009). Although both responsibility acceptance and sympathetic expression aim to lessen negative reactions, informing the public about corrective actions is also critical. In many states, data breach laws require the organization to inform affected individuals of potential risks associated with the incident and provide guidance on protecting from potential damage (i.e., use credit monitoring and identity theft protection services). Moreover, Bentley (2014) suggested that corrective actions are important to rebuilding organization-public relationships. Thus, future research should incorporate corrective actions into organizational apologies.

Findings in this study were limited to severe crises. Specifically, hypothesis two confirmed that either high or low sympathetic expression did not have significant effects on public responses. This is because sympathetic expression was recommended as an alternative option when crisis responsibility is perceived to be mild (Bennett & Ear walker, 2001). Thus, future research should examine the effects of sympathetic expression on public responses by comparing different crisis types (i.e., severe vs. moderate vs. mild crises).

Finally, the use of an experimental studies has its own limitations. Systematic manipulation and experiment control achieve internal validity, but limit the study's external validity. In other words, the generalizability to a broader array of populations is at risk because of various factors, such as artificial setting, participants' behaviors have no consequences and only have limited behavioral or other response options in the survey (Aronson, Ellsworth, Carlsmith, & Gonzales, 1990). Moreover, although MTurk provides a convenient platform to recruit eligible study participants, it was less reliable than normative or community-based samples (Rouse, 2015). This study also has short-term approach to long-term situation. Specifically, participants attended the survey once. However, in reality, individuals' reactions may change based on what an organization says in crisis communication messages and what it actually does (e.g., Niemann, Wisse, Rus, Van Yperen, & Sassenberg, 2014). Thus, future research could replicate this study using community-based samples and measure changes in individuals' reactions over time.

Conclusion

This study examined stakeholder perceptions of responsibility acceptance and sympathetic expression in different causal attributed conditions, and interaction effects of these three variables on public anger relief, organization's reputation, and trust in an organization's competence, benevolence, and integrity. The study results suggested that when a crisis is perceived as being caused by external/uncontrollable factor, individuals tend to have higher trust in an organization's competence and benevolence, and may feel less angry at the organization than a crisis incident caused by internal/controllable factors. This finding indicated that an organizational apology for a crisis caused by internal/controllable factor(s) needs more work in order to reduce stakeholders' feeling of anger and retain or regain their trust in the organization's knowledge, skills, and characteristics (competence) to handle the incident as well maintain the emotional and affective bonds and interactions between the organization and its stakeholders (benevolence).

Findings in this study also revealed that stakeholders perceive an apology with an explicit statement of responsibility acceptance differently from a simple apology with an implicit responsibility acceptance. This indicated that a simple apology does not always mean that an organization accepts responsibility. Thus, depending on the attributed crisis responsibility, an organization determines the extent to which it should accept responsibility. Crisis managers may use strategic ambiguity due to potential liability constrain if they choose to accept responsibility (Eisenberg, 1984). Additionally, the differences in stakeholder perceptions were found in organizational reputation and trust in an organization's competence, benevolence, and integrity. This result suggests that accepting responsibility appropriately could help an organization to regain a favorable reputational perception as well as appear to be trustworthy in terms of its competence, benevolence, and integrity. However, taking full responsibility (explicit responsibility acceptance) and a simple apology (implicit responsibility acceptance) appeared to have no different effects on relieving stakeholders' anger. Stakeholders probably expect a more detailed corrective actions to demonstrate how the organization plans to handle the issue when it claims to take responsibility. In other words, the use of strategic ambiguity in crisis responses may leave stakeholders dissatisfied, anger, and demand an apology (Tyler, 1997).

Findings in this study showed no different effect between high and low sympathetic expression in severe crises incidents. In other words, expressing sympathy would not suffice to handle severe crises. An organizational apology should include more components in order to address public concerns, reduce their anger, and regain their trust and favorable reputational perception. Finally, the interactions of causal attribution, responsibility acceptance, and sympathetic expression only yielded marginal significant difference on public anger relief. Stakeholders may expect a more rigorous apology with corrective actions in severe crises so they may regain their trust in the organization and restore a favorable perception of the organization's reputation.

References

Allcorn, S. (1994). *Anger in the workplace: Understanding the causes of aggression and violence*. Westport, CT: Greenwood.

Arnold, M. B. (1960). *Emotion and personality*. New York, NY: Columbia University Press.

Aronson, E., Ellsworth, P. C., Carlsmith, J. M., & Gonzales, M. H. (1990). *Methods of research in social psychology*. Boston, MA: McGraw-Hill.

Barrett-Lennard, G. T. (1962). Dimensions of therapist response as causal factors in therapeutic change. *Psychological monographs: General and applied*, *76*(43), 1.

Batson, C. D., Kennedy, C. L., Nord, L. A., Stocks, E. L., Fleming, D. Y. A., Marzette, C. M., & Zerger, T. (2007). Anger at unfairness: Is it moral outrage? *European Journal of Social Psychology*, *37*(6), 1272-1285.

Bennett, M., & Earwaker, D. (1994). Victims' responses to apologies: The effects of offender responsibility and offense severity. *The Journal of Social Psychology*, *134*(4), 457-464.

Benoit, W. L. (1995). *Accounts, excuses, and apologies*. Albany: State University of New York.

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177-186.

Benoit, W. L. (2015). *Accounts, excuses, and apologies (2nd ed.)*. Albany: State University of New York.

Benoit, W. L., & Brinson, S. L. (1999). Queen Elizabeth’s image repair discourse: Insensitive royal or compassionate queen? *Public Relations Review, 25*(2), 145-156.

Benoit, W. L., & Brinson, S. L. (1994). AT&T: Apologies are not enough. *Communication Quarterly, 42*(1), 75-88.

Benoit, W. L., & Czerwinski, A. (1997). A critical analysis of USAir's image repair discourse. *Busines Communication Quarterly, 60*(3), 38-57.

Benoit, W. L., & Drew, S. (1997). Appropriateness and effectiveness of image repair strategies. *Communication Reports*, *10*(2), 153-163.

Benoit, W. L., & Hanczor, R.S. (1994). The Tonya Harding controversy: An analysis of image restoration strategies. *Communication Quarterly, 42*(4), 416-433.

Bentley, J. M. (2014, November). Talk is cheap: Organizational apologies

from the stakeholder's perspective. Paper presented at the National

Communication Association (NCA) annual convention, Chicago, IL.

Bentley, J. M., Oostman, K. R., & Shah, S. F. A. (2018). We're sorry but it's not our fault: Organizational apologies in ambiguous crisis situations. *Journal of Contingencies and Crisis Management*, *26*(1), 138-149.

Brinson, S. L., & Benoit, W. L. (1996). Dow Corning's image repair strategies in the breast implant crisis. *Communication Quarterly, 44*(1), 29-41.

Brinson, S. L., & Benoit, W. L. (1999). The tarnished star: Restoring Texaco's damaged public image. *Management Communication Quarterly, 12*, 483-510.

Cacioppo, J. T., Petty, R. E., Feinstein, J. A., & Jarvis, B. G. W. (1996). Dispositional differences in cognitive motivation: The life and times of individuals varying in need for cognition. *Psychological Bulletin, 119*, 197-253.

Cannon, W. B. (1927). The James-Lange theory of emotions: A critical examination and an alternative theory. *The American journal of psychology*, *39*(1/4), 106-124.

Cannon, W. B. (1987). The James-Lange theory of emotions: a critical examination and an alternative theory. *The American journal of psychology*, *100*(3/4), 567-586.

Choi, Y., & Lin, Y. H. (2009). Individual difference in crisis response perception: How do legal experts and lay people perceive apology and compassion responses?. *Public relations review*, *35*(4), 452-454.

Chung, S. (2011). Corporate apology and crisis communication: The effect of responsibility admittance and sympathetic expression on public anger relief. *Graduate Theses and Dissertation*. 10248.

Chung, S., & Lee, S. (2017). Crisis Management and Corporate Apology: The Effects of Causal Attribution and Apology Type on Publics' Cognitive and Affective Responses. *International Journal of Business Communication*, 2329488417735646.

Claeys, A. S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the situational crisis communication theory and the moderating effects of locus of control. *Public Relations Review, 36,* 256-262.

Clifford, S. (2009, April 15). A video prank at Domino's taints brand. *The New York Times*. Retrieved from https://www.nytimes.com/2009/04/16/business/media/16dominos.html.

Cohen, J. R. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale, N.J.: Erlbaum Associates.

Cohen, J. R. (1999). Advising clients to apologize. *Southern California Law Review, 72,* 1009-1073.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *Journal of applied psychology*, *92*(4), 909.

Coombs, W.T. (1995). Choosing the right words: the development of guidelines for selection of the appropriate crisis-response strategies. *Management Communication Quarterly, 8*, 447-76.

Coombs, W. T. (2006). A theoretical frame for post-crisis communication. In M. J. Martinko (Ed.), *Attribution theory in the organizational sciences: Theoretical and empirical contributions* (pp. 275-296). Greenwich, CT: Information Age Publishing.

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. (2010). *Crisis communication: Planning, managing, and responding*. Thousand Oaks, CA: SAGE.

Coombs, W. T. (2013). Situational theory of crisis: Situational crisis communication theory and corporate reputation. In C. E. Carroll (Eds.), *The handbook of communication and corporate reputation* (pp. 262-278). John Wiley & Sons.

Coombs, W. T., & Holladay, S. J. (2002). 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., & Holladay, S. J. (2007). The negative communication dynamic: Exploring the impact of stakeholder affect on behavioral intentions. *Journal of Communication management*, *11*(4), 300-312.

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

Coombs, W., & Holladay, S. J. (2012). Amazon. com's Orwellian nightmare: exploring apology in an online environment. *Journal of Communication Management*, *16*(3), 280-295.

Coombs, T., & Schmidt, L. (2000). An empirical analysis of image restoration: Texaco's racism crisis. *Journal of Public Relations Research*, *12*(2), 163-178.

Courtright, J. L., & Hearit, K. M. (2002). The good organization speaking well: A paradigm case for religious institutional crisis management. *Public Relations Review*, *28*(4), 347-360.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches.* SAGE Publications.

Darby, B. W., & Schlenker, B. R. (1982). Children's reactions to apologies. *Journal of personality and social psychology*, *43*(4), 742.

Darley, J. M., & Pittman, T. S. (2003). The psychology of compensatory and retributive justice. *Personality and Social Psychology Review*, *7*(4), 324-336.

Diers-Lawson, A., & Pang, A. (2016). Did BP Atone for its Transgressions? Expanding Theory on ‘Ethical Apology in Crisis Communication. *Journal of Contingencies and Crisis Management*, *24*(3), 148-161.

DiStaso, M. W., Vafeiadis, M., & Amaral, C. (2015). Managing a health crisis on Facebook: How the response strategies of apology, sympathy, and information influence public relations. *Public Relations Review, 41*, 222-231.

Edwards, J. (2010, September 9). Self-flagellation as corporate strategy: Domino's "We suck!" campaign piles on the sales. *CBSNews*. Retrieved from https://www.cbsnews.com/news/self-flagellation-as-corporate-strategy-dominos-we-suck-campaign-piles-on-the-sales/

Eisenberg, E. M. (1984). Ambiguity as strategy in organizational communication. *Communication monographs*, *51*(3), 227-242.

Englehardt, K. J., Sallot, L. M., & Springston, J. K. (2004). Compassion without blame: Testing the accident decision flow chart with the crash of ValuJet Flight 592. *Journal of Public Relations Research*, *16*(2), 127-156.

Falkheimer, J., & Heide, M. (2015). Trust and brand recovery campaigns in crisis: Findus Nordic and the horsemeat scandal. *International Journal of Strategic Communication*, *9*(2), 134-147.

Ferrin, D. L., Kim, P. H., Cooper, C. D., & Dirks, K. T. (2007). Silence speaks volumes: the effectiveness of reticence in comparison to apology and denial for responding to integrity-and competence-based trust violations. *Journal of Applied Psychology*, *92*(4), 893.

Fombrun, C.J. (1996). *Reputation: Realizing Value from the Corporate Image*. Boston, MA: Harvard Business School Press.

Frandsen, F. & Johansen, W. (2010). Apologizing in a globalizing world: Crisis communication and apologetic ethics. *Corporate Communication: An International Journal, 15*(4), 350-364.

Frantz, C. M., & Bennigson, C. (2005). Better late than early: The influence of timing on apology effectiveness. *Journal of Experimental Social Psychology*, *41*(2), 201-207.

Freimuth, V. S., Musa, D., Hilyard, K., Quinn, S. C., & Kim, K. (2014). Trust during the early stages of the 2009 H1N1 pandemic. *Journal of health communication*, *19*(3), 321-339.

Fuchs-Burnett, T. (2002). Mass public corporate apology. *Dispute Resolution Journal, 57*, 26-32.

Gabarro, J. (1978). The development of trust, influence, and expectations. In A. G. Athos & J. J. Gabarro (Eds.), *Interpersonal behavior: Communication and understanding in relation-ships* (pp. 290-303). Englewood Cliffs, NJ: Prentice Hall.

Gonodo-Madikizel, P. (2003). Remorse, forgiveness, and re-humanization: Stories form South Africa. *Journal of Humanistic Psychology*, *42*, 7-32.

Grappi, S., & Romani, S. (2015). Company post-crisis communication strategies and the psychological mechanism underlying consumer reactions. *Journal of Public Relations Research*, *27*(1), 22-45.

Griffin, M., Babin, B., & Darden, W. (1992). Consumer assessments of responsibility for product-related injuries: The impact of regulations, warnings, and promotional policies. *Advances in Consumer Research, 19*, 870-878.

Hearit, K.H. (2006). *Crisis Management by Apology: Corporate Responses to Allegations of Wrongdoing*. Mahwah, NJ: Lawrence Erlbaum.

Helder, F. (1958). *The psychology of interpersonal relations*. *New York*, NY: Psychology Press.

Hodgins, H. S., & Liebeskind, E. (2003). Apology versus defense: Antecedents and consequences. *Journal of Experimental Social Psychology*, *39*(4), 297-316.

Hon, L. C., & Grunig, J. E. (1999). *Guidelines for measuring relationships in public relations*. Institute for Public Relations.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion*. New Haven, CT: Yale University Press.

Identity Theft Resource Center. (2017). *2017 ITRC data breach report.* Retrieved from http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf

Izard, C.E. (1991). *The psychology of emotions.* New York: Basil Blackwell.

Jenkins, A., Anandarajan, M., & D'Ovidio, R. (2014). 'All that Glitters is not Gold': The Role of Impression Management in Data Breach Notification. *Western Journal of Communication*, *78*(3), 337-357.

Jorgensen, B. (1996). Components of consumer reaction to company-related mishaps: A structural equation model. *Advanced in Consumer Research, 23*, 346-351.

Kardash, C. M., & Noel, L. K. How organizational signals, need for cognition, and verbal ability affect text recall and recognition. *Contemporary educational psychology, 25*, 317-331.

Keppel, G. (1991). *Design and analysis: A researcher's handbook*. Prentice-Hall, Inc.

Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: the effects of apology versus denial for repairing competence-versus integrity-based trust violations. *Journal of applied psychology*, *89*(1), 104.

Kim, B., Johnson, K., & Park, S. Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, *4*(1), 1354525.

Kramer, R. M., & Lewicki, R. J. (2010). Repairing and enhancing trust: Approaches to reducing organizational trust deficits. *Academy of Management annals*, *4*(1), 245-277.

Lazare, A. (2004). *On apology*. New York, NY: Oxford University Press.

Lazarus, R. S. (1991). *Emotion and adaption*. New York, NY: Oxford University.

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.

Lee, S., & Chung, S. (2012). Corporate apology and crisis communication: The effect of responsibility admittance and sympathetic expression on public's anger relief. *Public Relations Review*, *38*(5), 932-934.

Lerner, H. (1990). *The dance of anger*. New York, NY: Harper & Row.

Lewicki, R. J., Polin, B., & Lount Jr, R. B. (2016). An exploration of the structure of effective apologies. *Negotiation and Conflict Management Research*, *9*(2), 177-196.

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

Liu, B. & Mehta, A. (2017, March). *The trust factor: Towards a comprehensive model for trust in crisis communication.* Paper presented at the International Crisis and Risk Communication Conference, Orlando, FL.

Lyon, L., & Cameron, G. T. (2004). A relational approach examining the interplay of prior reputation and immediate response to a crisis. *Journal of public relations research*, *16*(3), 213-241.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods, 1*, 130-149.

Mark, M., & Reichardt, C. (2004). Quasi-experimental and correlational designs. In C. Sansone, C. Morf, & A. T. Panter (Eds.), *The Sage handbook of methods in social psychology* (pp. 265-286). Thousand Oaks, CA: Sage Publications.

Maxwell, S. (2001). When to use MANOVA and significant MANOVAs and insignificant ANOVAs or vice versa. *Journal of Consumer psychology*, 29-30.

May, L. N., & Jones, W. H. (2007). Does hurt linger? Exploring the nature of hurt feelings over time. *Current Psychology: Developmental, Learning, Personality, Social, 25*, 245-256.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

McCann, E. (2017, April 14). United's apologies: A timeline. *The New York Times*. Retrieved from https://www.nytimes.com/2017/04/14/business/united-airlines-passenger-doctor.html

McCullough, M. E., Worthington Jr, E. L., & Rachal, K. C. (1997). Interpersonal forgiving in close relationships. *Journal of personality and social psychology*, *73*(2), 321.

McDonald, L. M., Sparks, B., & Glendon, A. I. (2010). Stakeholder reactions to company crisis communication and causes. *Public Relations Review, 36*, 263-271.

McGrath, M. (2014, January 10). Target data breach spilled info on as many as 70 million customers. *Forbes*. Retrieved from https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#4fad5548e795

Mercer, P. (1972). Sympathy and ethics: a study of the relationship between sympathy and morality with special reference to Hume's Treatise.

Meredith, L. S., Eisenman, D. P., Rhodes, H., Ryan, G., & Long, A. (2007). Trust influences response to public health messages during a bioterrorist event. *Journal of health communication*, *12*(3), 217-232.

Mitchell, M., Brown, K., Morris-Villagran, M., & Villagran, P. (2001). The effects of anger, sadness and happiness on persuasive message processing: A test of the negative state relief model. *Communication Monographs*, *68*(4), 347-359.

Myers, C. (2016). Myers, C. (2016). Apology, sympathy, and empathy: The legal ramifications of admitting fault in US public relations practice. *Public Relations Review*, *42*(1), 176-183.

Nadler, A., & Liviatan, I. (2006). Intergroup reconciliation: Effects of adversary's expressions of empathy, responsibility, and recipients' trust. *Personality and Social Psychology Bulletin*, *32*(4), 459-470.

Niemann, J., Wisse, B., Rus, D., Van Yperen, n. w., & Sassenberg, K. (2014). Anger and attitudinal reactions to negative feedback: The effects of emotional instability and power. *Motivation and Emotion, 38*(5), 687-699.

Neuman, W. L. (2013). *Social research methods: Qualitative and quantitative approaches*. Pearson Education.

Novaco, R. W. (1994). Anger as a risk factor for violent among the mentally disordered. In J. Monahan & H. Steadman (Eds.), *Violence and mental disorder: Development in risk assessment.* University of Chicago Press.

Ohbuchi, K., & Sato, K. (1994). Chidren's reactions to mitigating accounts: apologies, excuses, and intentionality of harm. *Journal of Social Psychology, 134*, 5-17.

Ohbuchi, K., Kameda, M., & Agarie, N. (1989). Apology as aggression control: its role in mediating appraisal of and response to harm. *Journal of personality and social psychology*, *56*(2), 219.

Pace, K. M., Fediuk, T. A., & Botero, I. C. (2010). The acceptance of responsibility and expressions of regret in organizational apologies after a transgression. *Corporate Communications*, 15, 410–427.

Park, J., Cha, M., Kim, H., & Jeong, J. (2012). Managing bad news in social media: A case study on Domino's Pizza crisis. *ICWSM, 12*, 282-289.

Patel, A., & Reinsch, L. (2003). Companies can apologize: Corporate apologies and legal liability. *Business Communication Quarterly, 66*, 9-25.

Pfarrer, M. D., Decelles, K. A., Smith, K. G., & Taylor, M. S. (2008). After the fall: Reintegrating the corrupt organization. *Academy of Management Review*, *33*(3), 730-749.

Privacy Right Clearing House. Oct 2, 2017. *Data breaches.* Retrieved from https://www.privacyrights.org/data-breaches?title=&taxonomy_vocabulary_11_tid%5B%5D=2434

Reynolds, B.M Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative framework. *Journal of Health Communication, 10*, 43-55.

Robbennolt, J. K. (2009). Apologies and medical error. *Clinical Orthopaedics and Related Research, 467*(2), 376-382.

Rode, L. (2007). Database security breach notification statues: Does placing the responsibility on the true victim increase data security? *Houston Law Review, 43,* 1597-1634.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256-286.

Rosenbaum, T. (2004). The myth of moral justice. *Tikkun*, *19*(3), 65-69.

Scher, S. J., & Darley, J. M. (1997). How effective are the things people say to apologize? Effects of the realization of the apology speech act. *Journal of Psycholinguistic Research, 26*, 127-140.

Schlenker, B. R., & Darby, B. W. (1981). The use of apologies in social predicaments. *Social Psychology Quarterly, 44*, 271–278.

Schweitzer, M. E., Brooks, A. W., & Galinsky, A. (2015). The organization apology. *Harvard Business Review, September,* 44-52.

Smith, B. A. & Dillard, J. P. (1997, November). *Affect and persuasion: Evidence for cognitive coloration of message production.* Paper presented at the Annual Meeting of the National Communication Association, Chicago, Il.

Spence, P. R., Sellnow-Richmond, D. D., Sellnow, T. L., & Lachlan, K. A. (2016). Social media and corporate reputation during crises: The viability of video-sharing websites for providing counter-messages to traditional broadcast news. *Journal of Applied*

Communication Research, 44(3), 199-215.

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

Takuku, S. (2001). The effects of apology and perspective taking on interpersonal forgiveness. *Journal of Social Psychology, 141,* 494-508.

Tavuchis, N. (1991). *Mea culpa: A sociology of apology and reconciliation*. Stanford, CA: Stanford University Press.

Thomas, R. L., & Millar, M. G. (2008). The impact of failing to give an apology and the need-for-cognition on anger. *Current Psychology*, *27*(2), 126-134.

Tomlinson, E. C., Dineen, B. R., & Lewicki, R. J. (2004). The road to reconciliation: Antecedents of victim willingness to reconcile following a broken promise. *Journal of Management*, *30*(2), 165-187.

Tomlinson, E. C., & Mryer, R. C. (2009). The role of causal attribution dimensions in trust repair. *Academy of Management Review*, *34*(1), 85-104.

Taylor, M. (2000). Cultural variance as a challenge to global public relations: A case study of the Coca-Cola scare in Europe. *Public Relations Review*, *26*(3), 277-293.

Tyler, L. (1997). Liability means never being able to say you're sorry: Corporate guilt, legal constraints, and defensiveness in corporate communication. *Management communication quarterly*, *11*(1), 51-73.

Van Der Merwe, A. W., & Puth, G. (2014). Towards a conceptual model of the relationship between corporate trust and corporate reputation. *Corporate reputation review*, *17*(2), 138-156.

Van Laer, T., & de Ruyter, K. (201). In stories we trust: How narrative apologies provide cover for competitive vulnerability after integrity-violating blog posts. *International Journal of Research in Marketing, 27*, 164-174.

Victor, D., & Stevens, M. (2017, April 10). United airlines passenger is dragged from an overbooked flight. *The New York Times.* Retrieved from https://www.nytimes.com/2017/04/10/business/united-flight-passenger-dragged.html

Veltsos, J. R. (2012). An analysis of data breach notifications as negative news. *Business Communication Quarterly*, *75*(2), 192-207.

Verhoeven, J. W., Van Hoof, J. J., Ter Keurs, H., & Van Vuuren, M. (2012). Effects of apologies and crisis responsibility on corporate and spokesperson reputation. *Public Relations Review*, *38*(3), 501-504.

Weiner, B. (Ed.). (1974). *Achievement motivation and attribution theory*. General Learning Press.

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

Weiner, B. (2006). *Social movement, justice, and the moral emotions: An attribution approach*. Mahwah: Lawrence Erlbaum Associates.

Weiner, B., Graham, S., Peter, O., & Zmuidinas, M. (1991). Public confession and forgiveness. *Journal of Personality*, *59*(2), 281-312.

Weiss, A. M., Anderson, E., & MacInnis, D. J. (1999). Reputation management as a motivation for sales structure decisions. *The Journal of Marketing*, 74-89.

Williams, M. (2001). In whom we trust: Group membership as an affective context for trust development. *Academy of management review*, *26*(3), 377-396.

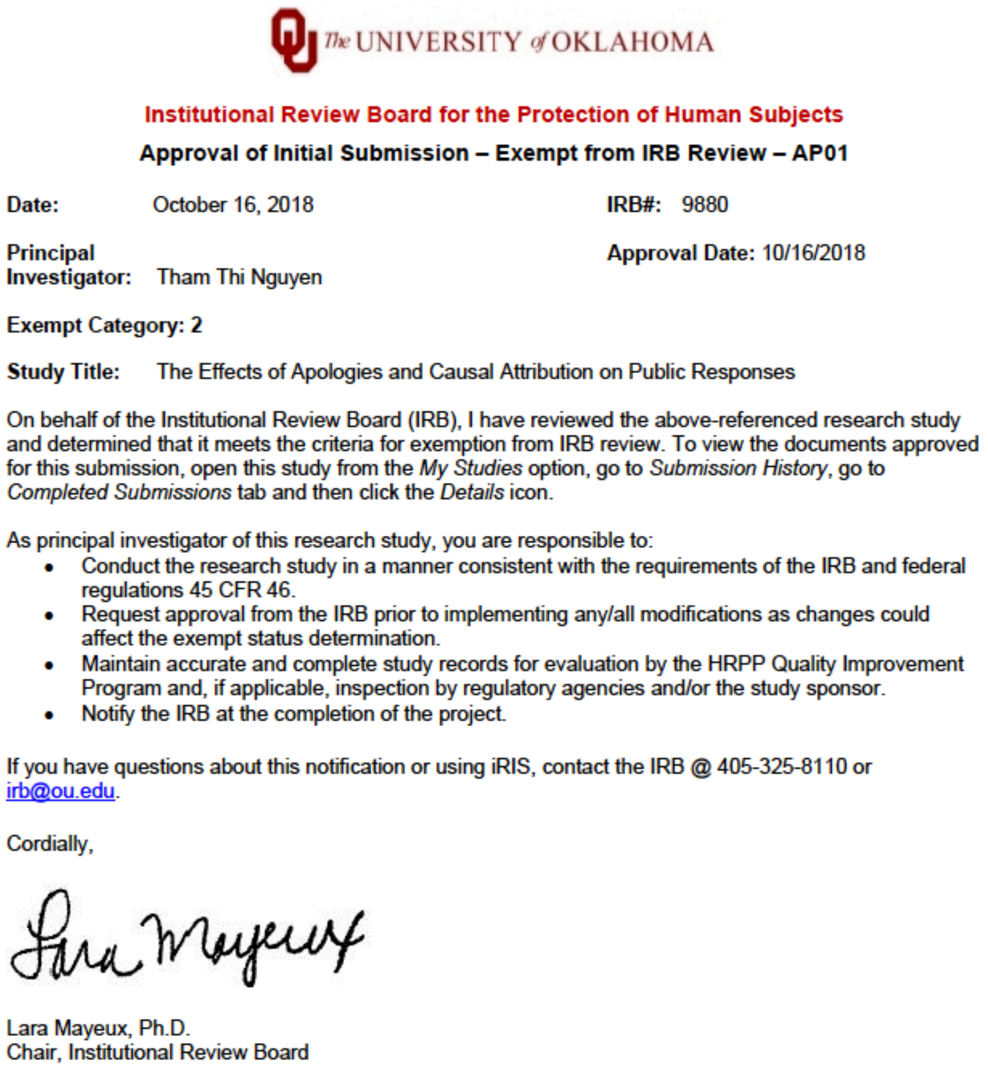
Wimmer, R. D., & Dominick, J. R. (2013). *Mass media research*. Cengage Learning.

Wispé, L. (1986). The distinction between sympathy and empathy: To call forth a concept, a word is needed. *Journal of personality and social psychology*, *50*(2), 314.

Zand, D. E. (1972). Trust and managerial problem solving. *Administrative Science Quarterly, 17,* 229-239.

Appendix A

Institutional Review Board Approval Letter



The UNIVERSITY of OKLAHOMA

Institutional Review Board for the Protection of Human Subjects

Approval of Initial Submission – Exempt from IRB Review – AP01

Date: October 16, 2018		**IRB#:** 9880
Principal Investigator: Tham Thi Nguyen		**Approval Date:** 10/16/2018

Exempt Category: 2

Study Title: The Effects of Apologies and Causal Attribution on Public Responses

On behalf of the Institutional Review Board (IRB), I have reviewed the above-referenced research study and determined that it meets the criteria for exemption from IRB review. To view the documents approved for this submission, open this study from the *My Studies* option, go to *Submission History*, go to *Completed Submissions* tab and then click the *Details* icon.

As principal investigator of this research study, you are responsible to:

- Conduct the research study in a manner consistent with the requirements of the IRB and federal regulations 45 CFR 46.
- Request approval from the IRB prior to implementing any/all modifications as changes could affect the exempt status determination.
- Maintain accurate and complete study records for evaluation by the HRPP Quality Improvement Program and, if applicable, inspection by regulatory agencies and/or the study sponsor.
- Notify the IRB at the completion of the project.

If you have questions about this notification or using iRIS, contact the IRB @ 405-325-8110 or irb@ou.edu.

Cordially,

Lara Mayeux

Lara Mayeux, Ph.D.
Chair, Institutional Review Board

Appendix B

Conditions for Each Independent Variable

Condition for Independent Variables	Manipulation
Responsibility acceptance	
Explicit	We are truly sorry for the inconvenience this incident may cause you. We're taking this incredibly seriously and accept responsibility to fix this security problem.
Implicit	We are truly sorry for the inconvenience this incident may cause you.
None (no message)	
Expression of sympathy	
High	We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.
Low	We know this breach has had a real impact on you, creating a great deal of confusion and frustration.
Causal attribution	
External	**We, TechBuy, invest $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer**

	information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration data and CVV (card verification value).
Internal	Our company, TechBuy, recently discovered that **we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption leys. Hackers stole that master keys and attacked our company encrypted data stored on Amazon's servers and gained hackers breached one of our systems and gained access to customer information**, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration data and CVV (card verification value).

Appendix C

News Article

TechBuy Data Breach Spilled Info On As Many As 10 Million Customers

Dakota McGrath, BBC Staff

TechBuy on Tuesday, October 16 confirmed the number of customers whose personal information was stolen in a widespread data breach between October 1 and October 15, 2018, reporting as many as 10 million customers.

In a statement, TechBuy said that information stolen included customer names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value). The retailer said that much of this data is "partial in nature," but it will nonetheless provide one year of free credit monitoring and identity theft protection to all customers who shopped at its U.S. stores.

"I want our customers to know that understanding and sharing the facts related to this incident is important to me and the entire TechBuy team," said Dakota Craig, TechBuy's chairman, president and CEO.

TechBuy generated revenue of more than $42 billion in fiscal 2018. At this time, the retailer said, it is not able to estimate the full cost to the company related to the data breach. However, all of these costs could affect TechBuy's 2018 business results and beyond.

About TechBuy

Seattle-based TechBuy Corporation (NYSE: TBC) serves customers at more than 1,000 large-format stores in the United States and at TechBuy.com since 1986. For the latest store count or more information, visit TechBuy.com/Pressroom. For a behind-the-scenes look at TechBuy, visit TechBuy.com/eyeview or follow @TechBuyNews on Twitter.

Appendix D

Stimuli

Group 1: A statement with external causal attribution, high sympathetic expression, and full responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

We, TechBuy, invested $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.

We are truly sorry for the inconvenience this incident may cause you. We're taking this incredibly seriously and accept full responsibility to fix this security problem.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 2: *A statement with internal causal attribution, high sympathetic expression, and explicit responsibility acceptance.*

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

Our company, TechBuy, recently discovered that we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption keys. Hackers stole that master keys, attacked our company encrypted data stored on Amazon's servers, and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.

We are truly sorry for the inconvenience this incident may cause you. We're taking this incredibly seriously and accept full responsibility to fix this security problem.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 3: A statement with external causal attribution, low sympathetic expression, and explicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

We, TechBuy, invested $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration.

We are truly sorry for the inconvenience this incident may cause you. We're taking this incredibly seriously and accept full responsibility to fix this security problem.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 4: A statement with internal causal attribution, low sympathetic expression, and full responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

Our company, TechBuy, recently discovered that we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption keys. Hackers stole that master keys, attacked our company encrypted data stored on Amazon's servers, and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration.

We are truly sorry for the inconvenience this incident may cause you. We're taking this incredibly seriously and accept full responsibility to fix this security problem.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 5: A statement with external causal attribution, high sympathetic expression, and implicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

We, TechBuy, invested $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.

We are truly sorry for the inconvenience this incident may cause you.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 6: A statement with internal causal attribution, high sympathetic expression, and implicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

Our company, TechBuy, recently discovered that we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption keys. Hackers stole that master keys, attacked our company encrypted data stored on Amazon's servers, and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card’s expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.

We are truly sorry for the inconvenience this incident may cause you.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 7: A statement with external causal attribution, low sympathetic expression, and implicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

We, TechBuy, invested $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration.

We are truly sorry for the inconvenience this incident may cause you.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 8: A statement with internal causal attribution, low sympathetic expression, and implicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

Our company, TechBuy, recently discovered that we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption keys. Hackers stole that master keys, attacked our company encrypted data stored on Amazon's servers, and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration.

We are truly sorry for the inconvenience this incident may cause you.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 9: A statement with external causal attribution, high sympathetic expression, and no statement of responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

We, TechBuy, invested $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 10: A statement with internal causal attribution, high sympathetic expression, and no statement of responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

Our company, TechBuy, recently discovered that we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption keys. Hackers stole that master keys, attacked our company encrypted data stored on Amazon's servers, and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration. We share those feelings. You expect more from us and deserve better.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 11: A statement with external causal attribution, low sympathetic expression, and implicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

We, TechBuy, invested $10 million every year to strengthen our cybersecurity system to keep our customers' information secure. However, we recently discovered that hackers breached one of our systems and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Group 12: A statement with internal causal attribution, low sympathetic expression, and implicit responsibility acceptance.

An Open Letter from CEO TechBuy

October 16, 2018

Dear TechBuy Customers,

Our company, TechBuy, recently discovered that we mistakenly left our data storage across four unsecured cloud servers, hosted on Amazon's S3 storage service, exposing highly sensitive passwords and decryption keys. Hackers stole that master keys, attacked our company encrypted data stored on Amazon's servers, and gained access to customer information, including your names, mailing addresses, phone numbers, email addresses, credit or debit card number, the card's expiration date and CVV (card verification value).

We know this breach has had a real impact on you, creating a great deal of confusion and frustration.

Sincerely,

Dakota Craig

Chairman, president and chief executive officer, TechBuy

Appendix E

Questionnaires for Preliminary Test

1. Hackers, not TechBuy, are responsible for the crisis.

   1. Strongly disagree …………………….. 7. Strongly agree

2. The blame for the crisis lies in the hackers, not TechBuy.

   1. Strongly disagree …………………….. 7. Strongly agree

3. The cause of the crisis is something TechBuy could control.

   1. Strongly disagree …………………….. 7. Strongly agree

4. The cause of the crisis is something that was manageable by TechBuy.

   1. Strongly disagree …………………….. 7. Strongly agree

5. The cause of the crisis is something over which TechBuy had power.

   1. Strongly disagree …………………….. 7. Strongly agree

6. How well does the message from TechBuy express sympathy toward the victims?

   a. Very well b. Not very well

7. How clearly does the message from TechBuy show that they took responsibility for the crisis?

   a. Implied b. Strongly agree

Demographic information

8. You are: □Male □ Female □ Rather not say

9. Age:_______________

10. Education: □Freshman □Sophomore □Junior □Senior □Graduate student

Appendix F

Questionnaires for Main Study

Screening questions:

Thanks for your interest in this survey. All of your replies will be kept strictly confidential.

1. Please indicate your employment status

   □ Homemaker/at home

   □ Unemployed/seeking employment

   □ Employed full time (35 hours or more per week)

   □ Employed part time (less than 34 hours per week)

   □ Freelance/self-employed

   □ Retired

   □ Full-time student

   □ Part-time student

2. How long have you been in the workforce (number of full-time employment only)?

   □ Less than 6 months

   □ Less than 3 years

   □ 4-10 years

   □ 11-15 years

   □ 16-20 years

   □ 21-25 years

   □ More than 25 years

3. What is your age?

☐ Under 30

☐ 30 to 34

☐ 35 to 39

☐ 40 to 44

☐ 45 to 49

☐ 50 to 54

☐ 55 to 59

☐ 60 to 64

This study seeks to understand your opinion about a data breach incident happened to TechBuy. TechBuy, a giant American consumer electronic retailer, discovered that cyber attackers had stolen information related to as many as 10 million customers between October 1 and October 15, 2018. Please read the news article in the next page and answer the questions that follow. (see Appendix B).

If you were among TechBuy's customers who personally identifiable information was compromised in this incident, what would be your reactions to TechBuy?
Please choose one of the options ranging from "1-Not at all" to "7-Very much" that best represents your reaction.

4. To what extent do you feel *mad* toward TechBuy?

   1. Not at all ……………………………… 7. Very much

5. To what extent do you feel *irritated* toward TechBuy?

   1. Not at all ……………………………… 7. Very much

6. To what extent do you feel *annoyed* toward TechBuy?

   1. Not at all ……………………………… 7. Very much

7. To what extent do you feel *angry* toward TechBuy?

    1. Not at all ……………………………… 7. Very much

8. To what extent do you feel *outraged* toward TechBuy?

    1. Not at all ……………………………… 7. Very much

On Tuesday, October 16, 2018, TechBuy notified these customers of the breach via email and letter. The text of the statement (notification letter) is as follows. Please read it and answer the questions in the next page. (see Appendix C).

To what extent do you agree or disagree with each of the following statements? **Please choose one of the options ranging from "1-Strongly disagree" to "7-Strongly agree" that best represents your reaction.**

9. Hackers, not TechBuy, are responsible for the crisis.

    1. Strongly disagree ……………………………… 7. Strongly agree

10. The blame for the crisis lies in the hackers, not TechBuy.

    1. Strongly disagree ……………………………… 7. Strongly agree

11. The cause of the crisis is something TechBuy could control.

    1. Strongly disagree ……………………………… 7. Strongly agree

12. The cause of the crisis is something that was manageable by TechBuy.

    1. Strongly disagree ……………………………… 7. Strongly agree

13. The cause of the crisis is something over which TechBuy had power.

    1. Strongly disagree ……………………………… 7. Strongly agree

14. The statement from TechBuy highly expressed sympathy toward the victims.

    1. Strongly disagree ……………………………… 7. Strongly agree

15. The statement from TechBuy clearly stated that they took responsibility for the crisis.

1. Strongly disagree ……………………………… 7. Strongly agree

16. The statement from TechBuy implied that they took responsibility for the crisis.

1. Strongly disagree ……………………………… 7. Strongly agree

17. The statement from TechBuy showed that they did not take responsibility for the crisis.

1. Strongly disagree ……………………………… 7. Strongly agree

After reading the statement from TechBuy, what would be your reactions with TechBuy? Please choose one of the options ranging from "1-Not at all" to "7-Very much" that best represents your reaction.

18. To what extent do you feel mad toward TechBuy?

1. Not at all ……………………………… 7. Very much

19. To what extent do you feel irritated toward TechBuy?

1. Not at all ……………………………… 7. Very much

20. To what extent do you feel annoyed toward TechBuy?

1. Not at all ……………………………… 7. Very much

21. To what extent do you feel angry toward TechBuy?

1. Not at all ……………………………… 7. Very much

22. To what extent do you feel outraged toward TechBuy?

1. Not at all ……………………………… 7. Very much

After reading the news article and statement from TechBuy, to what extent do you agree or disagree with each of the following statements? Please choose one of the options ranging from "1-Strongly disagree" to "7-Strongly agree" that best represents your reaction.

23. TechBuy is a *highly-regarded* company.

1. Strongly disagree …………………….. 7. Strongly agree

24. TechBuy is a *successful* company.

1. Strongly disagree …………………….. 7. Strongly agree

25. TechBuy is a *well-established* company

1. Strongly disagree …………………….. 7. Strongly agree

26. TechBuy seems to be *capable of* protecting consumer's identity.

1. Strongly disagree …………………….. 7. Strongly agree

27. TechBuy seems to be *known to be successful* at protecting consumers' identity.

1. Strongly disagree …………………….. 7. Strongly agree

28. TechBuy *seems to have much knowledge* about handling data breaches.

1. Strongly disagree …………………….. 7. Strongly agree

29. TechBuy seems to have *skills* in protecting consumers' identity.

1. Strongly disagree …………………….. 7. Strongly agree

30. TechBuy seems to have *specialized capacities* to protect consumers' identity.

1. Strongly disagree …………………….. 7. Strongly agree

31. TechBuy seems to be *qualified* in handling its data breach.

1. Strongly disagree …………………….. 7. Strongly agree

32. TechBuy is very concerned with my welfare.

1. Strongly disagree …………………….. 7. Strongly agree

33. My needs and desires are very important to TechBuy.

1. Strongly disagree …………………….. 7. Strongly agree

34. TechBuy would not knowingly do anything to hurt me.

1. Strongly disagree …………………….. 7. Strongly agree

35. TechBuy really looks out for what is important to me.

1. Strongly disagree …………………….. 7. Strongly agree

36. TechBuy will go out of its way to protect my identity from the data breach.

1. Strongly disagree …………………….. 7. Strongly agree

37. TechBuy has a strong sense of justice.

1. Strongly disagree …………………….. 7. Strongly agree

38. I never have to wonder whether TechBuy will stick to their word.

1. Strongly disagree …………………….. 7. Strongly agree

39. TechBuy tries hard to be fair in dealing with others.

1. Strongly disagree …………………….. 7. Strongly agree

40. TechBuy's actions and behaviors are not very consistent.

1. Strongly disagree …………………….. 7. Strongly agree

41. I like TechBuy's values.

1. Strongly disagree …………………….. 7. Strongly agree

42. Sound principles seem to guide TechBuy's behavior.

1. Strongly disagree …………………….. 7. Strongly agree

Demographic questions

43. What is your gender?

□ Male □ Female

44. Which of the following best describes you?

□ African American

□ Asian

□ Caucasian

□ Hispanic/Latino

☐ Native American or Alaskan Native

☐ Native Hawaiian or Pacific Islander

☐ Two or More Races/Others

45. What is the highest education level you have completed to date?

☐ Some high school or less

☐ High school graduate or equivalent

☐ Some college

☐ 2-year college graduate

☐ 4-year college graduate

☐ Some post-graduate

☐ Post-graduate degree

☐ Prefer not to answer

46. Which of the following best describes the industry you work in?

☐ Advertising

☐ Communications

☐ Construction

☐ Education

☐ Finance

☐ Health care

☐ Insurance

☐ Investment

☐ Manufacturing

☐ Market Research

□ Real estate

□ Retail

□ Sales

□ Technology

□ Other: please specify: ……

47. Which of the following best describes your total annual household income before taxes?

□ Under $35,000

□ $35,000 to $49,999

□ $50,000 to $74,999

□ $75,000 to $99,999

□ $100,000 to $149,999

□ $150,000 to $199,999

□ $200,000 or more

□ Prefer not to answer

48. How many debit and credit cards do you have?

□ None

□ 1

□ 2

□ 3

□ 4 or more

49. What is your relationship status?

□ Single or never married

□ Married or domestic partnership

□ Widowed

□ Divorced

□ Separated

50. Including yourself, how many people live your household? ……….

51. How many children under 18 currently live in your household?

□ None

□ 1

□ 2

□ 3

□ 4 or more

We received your response. Thank you for your participation!