universität wien

# MASTERARBEIT / MASTER’S THESIS

Titel der Masterarbeit / Title of the Master‘s Thesis

## „Exploring Stakeholder Perceptions of Apology in Preventable and Victim Organizational Crisis“

verfasst von / submitted by

Elene Koridze

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2022 / Vienna 2022

| | |
|---|---|
| Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet: | UA 066 841 |
| Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet: | Masterstudium Publizistik- und Kommunikationswissenschaft |
| Betreut von / Supervisor: | Univ.-Prof. Dr. Sabine Einwiller |

## Table of Contents

# 1 Introduction

Organizations are vulnerable to unpredictable crisis. When a crisis happens, organizations usually apologize for the situation, admit their mistakes and attempt to relieve public anger to protect and restore the organization's reputation. Therefore, how to apologize during a crisis situation is an important issue to organizations.

Coombs/Holladay (2010) define crisis management as: "A set of factors designed to combat crises and to lessen the actual damages inflicted. [It] seeks to prevent or lessen the negative outcomes of a crisis and thereby protect the organization, stakeholders, and/or industry from damage" (p.20). Communication is inevitable part of crisis management. A crisis or sometimes the threat of crisis creates an urge for information. Through communication, the information is collected, processed into knowledge, and finally shared with others. Communication is crucial in the entire crisis management process (p.25).

A crisis management can be divided into three categories: pre-crisis, crisis, and post-crisis. The precrisis stage involves three substages: signal detection, prevention, and crisis preparation. Organization should take appropriate measures to prevent crises. In the precrisis stage organization is oriented on specific action that will prevent crisis. However, there are some situations when crisis is not preventable, that is why organization members must be prepared. The third category, a postcrisis and actions related to it, help with the readiness for the next crisis. Besides, this phase is there to ensure the positive impression of the that stakeholders and to guarantee the actual end of the crisis (Coombs & Holladay, 2010, p.11-12).

According to Coombs/Holladay, along with these three categories, it is helpful to differentiate between two basic types of crisis communication: crisis knowledge management and stakeholder reaction management. As the authors note: "Crisis knowledge management involves identifying sources, collecting information, analyzing information, sharing knowledge, and decision making" (p.25). Besides, the authors state that the management is not visible to the public eye and the responses are created that send messages to its stakeholders. The public reaction management, moreover, "comprises communicative efforts (words and actions) to influence how stakeholders perceive the crisis, the organization in crisis, and the organization's crisis response" (p.25).

According to Coombs (2012), "a crisis is the perception of unpredictable event that threatens important expectancies of stakeholders" (p.2). Henceforce, it can be suggested that a crisis has a powerful potential to harm organization's reputation seriously, which will be reflected negatively on organizations success. From simply being prepared for emergency situations, crisis management has moved away from this and now includes for interconnected aspects: prevention, preparedness, response, and revision (p.5).

The crisis response phase is the most heavily researched aspect of crisis communication. The point is that the way an organization communicates during a crisis with its´ stakeholders has a significant effect on the consequences of the crisis, including the number of injuries and the amount of reputational damage suffered by the organization (Coombs & Holladay, 2010 p.28).

During the crisis event, crisis managers must realize that the organization is in crisis and take appropriate actions. This phase has two substages: crisis recognition and crisis containment. Communication with stakeholders is of the foremost importance during a crisis. An organization communicates to stakeholders through its words and actions. (Coombs, 2012, p.12)

Concerning crisis communication, Coombs (2012) recommends being quick, consistent and open. It is important to take into consideration that crisis communication emerges in times of stress (p.140). It is also vital to consider that the media reports crisis very quickly. In many instances, stakeholders hear about the crisis occurring from media or online reports some time before they have been officially notified by an organization, which, consequentially, puts a company in a dire situation.

According to Friedman (2002), emergency room physicians talk about the 'golden hour'. Dr. R Adams Cowley coined the phase as he believed that the first hour was the most crucial one when treating a patient in an emergency situation – if he were to stop the bleeding and restore the blood pressure in this time-frame, he could actually save the patient. Using the analogy, crisis is often perceived like a medical emergency where the first hour is the most significant time to provide the stakeholders with the appropriate 'treatment', in this case crisis response.

As already mentioned, reputation of an organization is threatened during any crisis. There is a belief that communication affects how stakeholders perceive organization in crisis. Accordingly, a variety of crisis responses strategies have been identified by researchers. Besides, crisis type plays an important role in selecting appropriate strategies. Apologies are social constructs, which means that their performance and perception can changes over time. It also means that stakeholders play a vital role in determining what is or is not an acceptable organizational apology. As the recipients of apologies, customers are willing to accept an appropriate apology during a crisis. There is also very little research on apologies from the stakeholder perspective. This makes it hard for managers to know how an organization should apologize, which, in turn, increases the risk of inappropriate apologies offered, that might further offend the stakeholders.

As reported by Benoit (2014), there is no universally agreed conception of an apology. Apology can include explicit acceptance of blame, expression of regret or remorse, or a request for forgiveness. However, the phrase "I'm sorry" is vague. It can express an admission of guilt, as in "I'm sorry I hurt you," or it can be regarded as an expression of sympathy, as in "I'm sorry you have been hurt" (implicitly by someone else). Admitting blame is risky. Not only is it about admitting, but such an action has negative consequences to organization's reputation. There is always a hope that the receiving side will forgive of the misconduct, but such a forgiveness is never guaranteed (p.26).

Bentley (2018), in his study "What Counts as an Apology? Exploring Stakeholder Perceptions in a Hypothetical Organizational Crisis", examined stakeholders' perceptions in a hypothetical organizational crisis (weak attribution of crisis responsibility). He explored stakeholder perceptions in a hypothetical organizational crisis using a convenience sample and a single crisis type. The themes and categories identified in his study provided different possible elements for organizational apologies but may not be generalized to other crisis types.

Accordingly, it was crucial to examine stakeholders' perceptions of apologies in a victim as well as preventable organizational crisis. Furthermore, data breaches are ambiguous crises. In one sense, the organization is a victim of the hackers. In another sense, the organization has failed to safeguard customer information. What is more, it is critical to explore what attribution level do stakeholders regard an organisation to carry when a data breach occurs for different reasons, to further enrich the theoretical bases for the apology construction. Thus, the study presented below, examined whether there was a significant difference between the levels of crisis type (preventable vs. victim) as well as source of information (media vs. organization) considering the apologies written by stakeholders.

To briefly present the structure of the work, the following sections unfold as follows. The second chapter opens with the theoretical basis of this study which is mainly based on the Situational Crisis Communication Theory developed by Coombs and his colleagues (1995). The literature review in the same section,  addresses the concept of social legitimacy, value of reputation and an organizations' dependence on its´ stakeholders. It also discusses phenomena of stealing thunder, importance of apologies, and how they work to restore legitimacy and what elements they must include. As a next step, it poses three research questions that will be presented in this study. In the third chapter, the methodology and the research design will be discussed in detail. What follows, chapter four presents the findings of the research conducted and reviews the results of the factorial analysis (ANOVA). Finally, chapter five comprises of discussion, theoretical as well as practical implications, and limitations of the study. The very last section of the work presents some concluding remarks as well as ways and suggestions for future research.

## 2 Theoretical Basis

Many scholars studied the role of apologies in crisis communication. In 1995, Coombs and his colleagues developed one of the theories - Situational Crisis Communication Theory. The main concept of the theory is that crises are negative events and stakeholders make attributions about crisis responsibility. Those attributions, in turn, will affect how public interacts with the organization in crisis (Coombs &Holladay, 2010, p.38). This means that stakeholders have their own perception about the occurred crisis, who is to blame about the crisis and how the organization should behave to earn back their trust. According to Coombs/Holladay(2010):

> "SCCT is audience oriented because it seeks to illuminate how people perceive crises, their reactions to crisis response strategies, and audience reactions to the organization in crisis. The nature of the crisis situation shapes audience perceptions and attributions. Hence, efforts to understand how people perceive crisis situations are audience centered."
> The main aim is to understand how people make attributions about crises and the effects of those attributions on their attitudes and behavioral intentions (p.38)

The core of SCCT is crisis responsibility. Attributions of crisis responsibility have a significant effect on how people perceive the reputation of an organization in crisis and their affective and behavioral responses to that organization following the crisis. A crisis is a threat to an organization's reputation. Reputation matters because it is an important and intangible resource for an organization. Moreover, crises can generate negative affect and behavioral intentions toward an organization. Crisis responsibility is a major factor in determining the threat posed by a crisis (Coombs & Holladay, 2010, p.38).

A strategic communicative response protects the reputation resource by evaluating crisis situation and respectively selecting the response strategy that fits the situation. There are other concerns to be addressed in a crisis, particularly, public safety. Coombs/Holladay (2002) note that before coping with reputational threats there is a necessity of providing instructing information, which means showing the stakeholders ways to protect themselves in a crisis. According to the authors "the central focus of SCCT is how to manage organizational reputation during a crisis" (p.167). The decision regarding a crisis response starts with determining an appropriate approach to it through pinpointing the crisis type. The main aim is to evaluate the crisis attribution level and the ability of an organization to control the event. As Coombs/Holladay (2002) state: "Perceptions of crisis responsibility have proven to increase as attributions of personal control intensify. In fact, personal control and crisis responsibility may be so highly correlated as to merit treating them" (p.167).

SCCT introduces a two-step process for assessing the crisis threat. The first step is to determine the frame stakeholders are using to categorize the process. According to the theory, there are three types of crises: victim type of crisis, accidental crisis and intentional crisis. Victim type of crisis has low crisis responsibility, while minimal crisis responsibility is attributed to the accidental crisis. The intentional crisis comes with the most responsibility. The three categories represent increasing levels of attributions of crisis responsibility and threat posed by a crisis. Determining the crisis type establishes the base threat presented by the crisis. The second step is to determine if any of the two intensifying factors exist. The intensifying factors change attributions of crisis responsibility and intensify the threat from it. Currently, two intensifying factors have been documented: (1) crisis history and (2) prior reputation (Coombs & Holladay, 2010, p.39).

The Situational Crisis Communication Theory (SCCT) is one among the many evolving theories that applies attribution theory to crisis management. In public relations, the SCCT has used attribution theory to develop and test a set of recommendations for using crisis response strategies. Attribution theory is a social-psychological theory that attempts to explain how people make sense of events. The idea is that when an event happens, especially a negative event, people try to determine why the event occurred (Coombs & Holladay, 2010, p.37).

Weiner (1986) argued that when an event is negative, unexpected, or important, there is a possibility that people will engage in what he calls "causal attribution processing" (p.549). To explain causal attribution process, he created the concepts of locus and controllability as main casual attributes. Locus identifies the location of the cause of an event as internal or external to the offender. Controllability refers to whether the prevention of a crisis is within the control of the offender. According to Weiner (1986), "anger is elicited when a personal failure is caused by internally and controllable reasons. Failure is assigned to causes viewed as uncontrollable, pity is elicited.'' (p.548)

## 2.1 Social Legitimacy

Organizational legitimacy is the public's belief that an organization has "a right to exist and conduct operations" (Metzler, 2001, p. 322). Organizations must demonstrate that their values are congruent with those of the public in order to be perceived as legitimate (Dowling & Pfeffer, 1975). Without this, it will be extremely difficult for an organization to gather customer support as well as that of investors and donors and functioning as a whole might become challenging.

For Hearit (1995), a crisis is a threat to an organization's social legitimacy (the consistency between organizational values and stakeholder values). Stakeholders' can be disappointed since their expectations of how an organization should function will not be in sync with the reality, which, in turn, will make them doubt the social legitimacy of the organization itself. Corporate apologia strives for restoring social legitimacy.

Hearit (1995) stated that although corporations must stay financially viable and operate within the law, these actions solely are not sufficient to establish social legitimacy. Legitimacy also depends on "how a corporation's policy affects the larger social system in which it operates" (p.2). For the author, competence is the first pillar that corporation must achieve to maintain legitimacy. Besides, a corporation must meet socially constructed standards of quality and at the same time operate in accordance with accepted standards of professionalism. A social legitimacy crisis is a situation in which organization has violated normative standards of behavior (p.2 - 3).

## 2.2 Value of Reputation

According to Coombs (2012), organization can be seen as having favorable or unfavorable reputation. Practitioners and academic writers agree that a reputation is exceptionally valuable, however abstract organizational resource. Favorable reputations is directly connected to attracting customers and top employee talent, generating investment interest, motivating workers, increasing job satisfaction, generating more positive media coverage, and garnering positive comments from financial analysts. A reputation is built through the direct and indirect experiences stakeholders have with the organization (p.14).

Direct experience is when a customer goes into the store to buy a product. Using a service is also considered a direct experience. On the other hand, mediated contact is about word-of-mouth communication, online messages from the organization and others, as well as any article or media report about an organization. As Coombs/Holladay (2010) write, the aim of reputation management is to create more favorable impression in stakeholders. To achieve the above-mentioned, managers try to create positive points of contact with an organization, including favorable shopping experiences and word-of-mouth, positive publicity, and advertisements that feature "the good points" about an organization. "All the various points of contact with an organization are fused in a stakeholder's mind to create a mosaic that is the organization's reputation" (p.58). Positive interactions and information about the organization build favorable reputations. On the other hand, unpleasant interactions and negative information lead to unfavorable reputations. A crisis can be a threat to a reputational asset. "As greater emphasis is placed in reputation, a corresponding emphasis must be placed on crisis management as means of protecting a reputational asset" (Coombs, 2012, p.14).

## 2.3 Stakeholder theory

According to Clarkson (1995), "stakeholders are persons or groups that have, or claim, ownership, rights or interests in a corporation and activities, past, present or future" (p.107). Stakeholders who have similar rights, interests or claims, can be classified in the same group: employees, shareholders, customers, and so on. Without primary stakeholders groups, organizations cannot function. Primary stakeholder groups typically consist of shareholders, investors, employees, customers. Organizations and primary stakeholder groups depend on each other greatly. If any primary stakeholder group, for example customers or suppliers, decide not to cooperate further with the organization, company will be damaged seriously. Secondary stakeholders or influencers are those people or groups who can affect or be affected by organizations. Typical influencers are media, activist groups and competitors. Influencers cannot stop organization from functioning, but they can cause serious harm to organization (p.107-108).

As Lee (2004) noted, there was a need for crisis communication research to concentrate on the audience. The informal and transition research examine the messages the crisis managers create with the goal of effecting the audience. The formal crisis communication research is more audience oriented. The emphasis is on how the receivers/audience react to crisis events and crisis response strategies (p.601).

The best comparison of the sender and audience-oriented perspectives is the way formal crisis communication research studies the crisis response strategies - what crisis managers say and do after a crisis occurs. An important result of the informal and transition crisis communication research is inventing crisis response strategies. These crisis response strategies are used in formal, transition, and informal crisis research projects. The research generally has a sender orientation because the concern is with defining the crisis response strategies that the crisis manager (sender) might use. The formal research diverts attention to examining how receivers react to the crisis response messages (Coombs & Holladay, 2010. p.35).

Ferrell (2004) noted that customers are one of the most important stakeholder groups to any business, “they provide financial resources, loyalty, and enhanced reputation that can help create positive firm images” (p. 128). Businesses need to realize that customers “evaluate the ethical practices of companies” (p. 127) and may disassociate themselves from companies they perceive to be irresponsible. Although the best way to avoid problems is for an organization to act ethically and maintain good relationships with all stakeholders, this is not always possible. Therefore, when stakeholder interests or expectations are violated, an organization must assess its actions objectively and communicate with affected stakeholders to protect its reputation and resolve legitimacy. One way to do this is through apologizing.

### 2.4 Evaluating Reputational Threat

The SCCT instructs organizations how to communicate with their various stakeholders to maintain the relationship between itself and the public. In general, the theory develops four further situational factors that suggest the ways in which the reputation of an organization is directly and indirectly affected by those: (1) initial crisis responsibility (i.e. stakeholders' perceptions on an organization's personal control of a crisis which is contingent upon crisis types such as a victim, accident, or preventable crisis), (2) crisis history (i.e. presence or absence of a similar crisis in the past), (3) prior reputation (i.e. how an organization treat its publics in a past crisis), and (4) severity of a crisis (i.e. the scale of loss, disaster, injury or destruction caused by a crisis that can increase public evaluation of crisis responsibility). Here, crisis responsibility is defined as: "The degree to which stakeholders blame the organization for the crisis event" (Coombs, 1998, p.180).

As a way to repair organizational reputation, crisis communicators should identify a type of given crisis by evaluating the level of crisis responsibility which the crisis carries. In a victim cluster the organization is perceived as the victim of the crisis and it is attributed the weakest level of responsibility. In an accident cluster, the organization is considered as unintentionally causing the crisis and is attributed a minimal level of responsibility. In a preventable cluster the organization is blamed of causing the crisis and it is attributed the strongest level of crisis responsibility (Coombs, 2012, p.157).

Table 1. Crisis Types, by level of responsibility

| |
|---|
| **Victim Cluster: Very little attribution of crisis responsibility**<br>▪ Natural disaster<br>▪ Rumors<br>▪ Workplace violence<br>▪ Malevolence |
| **Accidental Cluster: Low attribution of crisis responsibility**<br>▪ Challenges<br>▪ Technical - error accidents<br>▪ Technical – error product harm |
| **Preventable Cluster: Strong attribution of crisis responsibility**<br>▪ Human – error accident<br>▪ Human – error product harm<br>▪ Organizational misdeeds |

(from Coombs, 2012, p.158)

The crisis type is recognized as an important factor in the process of selecting strategies. The main challenge is to understand when to use a particular strategy for a specific crisis. Attribution theory has been offered as a useful framework for fitting the crisis response to the crisis situation. The Situational Crisis Communication Theory (SCCT) is part of a growing body of research that applies attribution theory to crisis management. In public relations, the SCCT has used attribution theory to develop and test recommendations for using crisis response strategies. Attribution theory is a social-psychological theory that attempts to explain how people make sense of events. Central thought is that when a negative event happens people try to figure out the cause of this event. People will make attributions of responsibility for events based on limited evidence. The general attribution is that responsibility lies with the person involved in the event (internal) or environmental factors (external) (Coombs & Holladay, 2010, p.37).

According to Weiner (1986), one of the main supporters of attribution theory (AT), attributions of internal or external responsibility shape affective and behavioral responses to the person involved in the event. As Coombs/Holladay (2010) state, it is reasonable to extend AT to crisis communication. Stakeholders will make attributions of crisis responsibility. Thus, the following question can be asked: Is the cause of crisis organizational or environmental? The main aim of attribution theory is to understand the factors that form people's attributions and reactions about the crisis and that is what makes AT approaches audience oriented. Those attributions will shape affect and behaviors directed toward the organization in crisis (p.37). According to Coombs/Holladay (2010), "the AT-based crisis research is audience-centered because it attempts to understand how various factors in the crisis situation shape the crisis attributions stakeholders might make about the crisis" (p.37). The authors further write that the marketing literature is rich with usages of AT in cases of crisis, that, in turn, aid the SCCT. How to reform ideas into effective crisis communication is at the core of SCCT that is rooted in AT.

### 2.5 Apology

As reported by Kellerman (2006), apology is the most complex and controversial of the crisis response strategies. It is crucial to differentiate between full and partial apologies. A full apology must acknowledge the crisis, accept responsibility, include a promise not to repeat crisis, and concern and regret. A partial apology is typically just an expression of concern and regret (p.156).

According to Patel & Reinsch (2003), when a corporation has clearly committed an awful act, a more complete apology that acknowledges responsibility may be the more relevant choice. Such an apology might read as follows: ''We, ABC Corporation, acknowledge the fact of wrongdoing, accept full responsibility for our actions, and express od wrongdoing, accept full responsibility for our actions, and express sincere sorrow and regret'' (p.22). Crucial here is to differentiate between full and partial apology. The main aspect setting the two apart is the clear statement of fault of responsibility vividly present in the full apology. In the cases where the guilt is unavoidable, mitigating the damage of the act and trying to minimize the costs are the required options. Full apology should probably include some promise not to repeat the offence again and compensate when needed (p.22).

Besides, according to Patel/Reinsch (2003) apology is also socially significant since it not only concerns the relations among the organization and the stakeholders, but also the relationship between the offender and the wider public. Reintegration can be the consequence of the right apology, which will also minimize the adverse effects of the offence. By analogy, a corporation may also reintegrate itself with the community of consumers by offering an expression of remorse or sympathy to those harmed by its actions (p.28).

As Buckley & Eberts (1996) state, "the relationship of a company to its community is particularly relevant to the possibility of a class action" (p.18). If a company cannot deny wrongdoing, one of its greatest risks is a class action suit, in which all parties claiming injury may join together in a lawsuit. What is at stake in such cases is the many separate parties coming together to join their forces to form a joint case agains the company. In such circumstances, a lot of money, as well as, sometimes, the company's existence itself are at risk. However, by right measures and apology, corporations have more chance to avoid such cases. Revealing its own fault before others do so can put a corporation in the position to shape public response. It provides an opportunity to initiate defensive measures by providing context of history and future commitments to responsibility (Patel & Reinsch, 2003, p.18)

According to Hearit (2006), "no matter what type of crises an organization faces - be they allegations of accidents, scandals and illegalities, product safety incidents, or social irresponsibility - the fact of the matter is that apologies have common ritualistic foundations" (p.123). It is reasonable for organizations to face their wrongdoing, publicly address their guilt, and then request a return back into the social community. It does not matter what degree of guilt an organization carries; it must face the public criticism anyway and deal with the sanctions that comes with acknowledging the guilt. By offering an apology, companies are able to express their remorse and guilt, and together with corrective action find ways to reintegrate (p.123).

Researchers have emphasized the advantages of apology among a variety of crisis responses. For example, Thomas/Millar (2008) stated that apologies are an important part of social discourse and have a function of reducing anger. The need or desire for punishing an organization for their actions is less in cases of admitting responsibility and apologizing (Darby & Schlenker, 1989; Ohbuchi et al., 1989). Compared to other response strategies in crisis situations, an apology turns out to be the most effective way to reestablish the reputation and social legitimacy (Benoit, 1995; Benoit & Drew, 1997; Bradford & Garrett, 1995; Clays, Cauberghe, & Vyncke, 2010; Dean, 2004). Apologies can also play a significant role in how organizations respond to an angry public and criticisms to defend organization's image in the crisis (Benoit, 1995). Indeed, an apology has various benefits in a crisis, which makes it a frequently preferred crisis response strategy (Bradford & Garrett, 1995; Dean, 2004). For example, offering compensation serves as a way to restore organization's reputation. Empirically, it has been demonstrated that compensation can lead to a positive outcome on relieving anger (Coombs & Holladay, 2008). Courtright/Hearit (2002) also maintain that an apology can be effective when a statement of responsibility is combined with some form of compensation. As Lee and Chung (2012) found, there is also difference between active and passive responsibility. Stakeholders respond more negatively to the passive responsibility, as it can be perceived as defensive and morally unacceptable (p.932-934).

What constitutes an apology varies between scholars, but it is generally agreed that there are essential components to a complete corporate apology. First of all, many scholars acknowledge that a responsible statement can be a key component of apology to reduce the level of anger felt by victims (Cohen, 1999; Coombs & Holladay, 2008; Darby & Schlenker, 1982). According to Lazare (2004), when the the organization does not accept responsibility for occurred crisis, this can result in the apology being more destructive than when no apology is offered.

When organization apologizes, it accepts responsibility for the crisis. Compensation promotes the acceptance of responsibility by offering compensation in form of money. Finally, corrective action involves identifying and fixing the source of the crisis. Corrective action can also be seen as an acceptance of responsibility for a crisis, because when an organization identifies and then eliminates the cause of the crisis, this process can be seen as efforts from the side of organization to prevent reoccurrence of the crisis. Various studies find that corporate responses indicating acceptance of responsibility fostered more positive brand attitudes, a stronger corporate image, and more supportive behavior (Coombs & Schmidt, 2000).

Shuman (2000) advises full apologies to be meaningful, the wrongdoer must acknowledge responsibility and take appropriate steps to repair damage. If stakeholders were harmed greatly, for financial loss or a physical injury, the apology should be coupled with compensation. Timing of an apology is also crucial to its success and acceptance. The author further notes that: "The nearer the apology is to the event in question, the more likely that the apology will be regarded as sincere and result in positive consequences. This, wherever possible, apologies should be offered in a timely fashion" (p.186).

An organization's response to a crisis might give stakeholders an image  how the organization perceive its' responsibility. Quattrone (1982) argued that people often engage in "backward chaining" in which they analyze actions that occur after an action to infer what caused the action. This means that during organizational crisis stakeholders make conclusion from unknown truth about the crisis by observing crisis responses do find out crisis cause.

Accordingly, organizations response will have a great influence on how stakeholders perceive the organization and its attribution level to crisis. Consumers may regard a denial as a egoistical attempt to avoid blame and that action is blameworthy. Indeed, denial of responsibility for a negative event can elicit anger and aggression.

In contrast, an organization's acceptance of crisis responsibility may appear more honorable, which may reduce the likelihood of negative responses. Research has found that acceptance of responsibility for a negative event can increase sympathy and forgiveness (Weiner, Graham, Peter, & Zmuidinas, 1991).

It makes sense that when organizations violate social norms, they should apologize to their stakeholders. However, organizational apologies can be more complicated than individual apologies because guilt is often difficult to assign (Hearit, 2006). According to Bentley (2010), unlike individuals, organizations may not have one person who is clearly to blame. There may be systemic problems or patterns of poor behavior that turn into a crisis. There is possibility that members of the organization had nothing to do with crisis, however they must take responsibility for it. On the other hand, there may be managers who are so focused on the interests of stockholders that they ignore the damage done to other stakeholder relationships (p.206).

Accordingly, it must be suggested that although perception of apologies differ among scholars, one of the aspects they agree on is that an appreciate response from an organization after a crisis is of great importance and a proper apology can reduce anger in stakeholders. Furthermore, not just rebuilding reputation of organization, reestablishing its' social legitimacy and stabilizing relationships with customers is a huge advantage of a proper apology after a crisis, but it can also help organization to get rid of legal ramifications.

## 2.6 Stealing Thunder

According to Arpan & Pompper (2003): "In the framework of crisis communication, stealing thunder is an admission of a weakness (usually a mistake or failure) before that weakness is announced by another party, such as an interest group or the media" (p.295). Several important theoretical streams may explain why the stealing thunder crisis communication strategy works.

First, According to Brock/Brannon(1992), commodity theory which explains the efficiency of stealing thunder, suggests following: "Messages are just like commodities. The more of them there are, the less value they carry." (p.138). When an organization has made information fully available there is nothing left to journalists to write about. Besides, by competing to be first who discloses information, journalists may lose interest in covering the story - unless it is considered newsworthy for reasons other than conflict.

Audiences generally expect communicators to be influenced by situational factors that result in either a knowledge bias or a reporting bias. Knowledge bias assumes that communicators have limited or nonrepresentative information that prohibits their ability to convey the truth. Reporting bias assumes that communicators' willingness to accurately convey relevant information is somehow compromised. When communicators deliver information consistent with these biases, audiences perceive them as less persuasive. The converse also is true. Communicators who deliver information that violates expected biases are perceived as more credible and more persuasive. In such a case, audiences usually resolve that a highly compelling external reality caused the communicator to act out of character, making the message more believable (Hunt & Kernan, 1984).

According to Arpan/ Pompper (2003), among journalists who rely on public relations practitioners for information subsidies, many likely expect organizational spokespeople to exhibit both knowledge and reporting biases during crises. Practitioners who offer a quick self-disclosure could disconfirm reporters' expectancies, leading to increased credibility for the spokesperson and the organization, and result in greater acceptance of crisis communication messages. Therefore, stealing thunder may offer practitioners a key ingredient for developing strong relationships with journalists - credibility (Arpan & Pompper, 2003, p.295)

Another proposed theoretical explanation for the effectiveness of stealing thunder is "change of meaning." When an organization revels the truth about occurred crisis, journalist might try to change its´ meaning in accordance with their beliefs about the organization. This change of meaning" could result in journalists' discounting the importance of a message or downplaying a crisis' severity. (Hamilton & Zanna, 1974).

Accordingly, it can be suggested that timing and the way organization communicates with its stakeholders is vital for organizations' reputation. Suppression of the truth will bring organization to worse condition, as at some point the truth will be revealed and this way of disclosure will be unfavorable for organizations' reputation.

## 2.7 Data Breach

According to Kim et al. (2017), there is a little scholarly research concerning data breach and cyber crisis management issues in public relations and other related journals. Organizations facing data breaches should follow legal ramifications and communicate about the occurred crisis with all affected and potentially affected consumers whose data might have been compromised (p.3).

As Ayygari/Ramashkina (2012) noted, data breaches have become one of the biggest problems for organizations, costing an average of 7.2 million dollars per breach. Data breaches are commonly associated with hacking – however, it is worth mentioning that breaches due to hacking are decreasing. On the other hand, breaches due to "human element" are increasing. Organizations need to implement effective training and stricter enforcement of security policies (p.33).

For organizations, data breaches or the potential data breach are huge challenges. Any unauthorized access or inadvertent disclosure of sensitive information can have dire consequences. The organization can face fines due to regulatory compliance, legal action from consumers, increased expenditure for improving security, and loss of consumer trust (Ayyagari, Ramakrishna 2012, p.33).

Noteworthy, Ramakrishna (2012) argues that, recent data breaches are normally human errors (i.e., crises caused by careless employees in protecting consumer information, outdated security programs, and a lack of proper employee training and administrative security policies) (p.33)

## 2.8 Research questions

Apologies are social constructs that's why they may look different to people in different roles or situations. The concept of social legitimacy implies that stakeholders want organizations to hold the same basic values they hold. It is likely that stakeholders will look for indications in an organizational apology that the organization adheres to these common values. From an organization's perspective, an effective apology will help organizations to recover from the crisis by recapturing stakeholders' support. However, legal and financial concerns may limit what an organization is willing to say in its apology. Furthermore, if organizations do not recognize the value of all stakeholders, they may ignore certain stakeholder concerns when apologizing. (Bentley, 2018, p.211)

As already mentioned, every Scholar has their own definition of apology. When an organization's reputation or social legitimacy is threatened and its` relationship with key stakeholders is in jeopardy, the priority must be to communicate in ways that satisfy stakeholders' needs.

Accordingly, the study examined the following questions:

*Research question 1: What elements of an organizational apology are important in reestablishing social legitimacy with stakeholders in victim and preventable types of crisis?*

*Research question 2: Is there a significant difference between preventable and victim types of organizational crisis considering the apologies constructed by stakeholders?*

According to Arpan/Pompper (2003): "In the framework of crisis communication, stealing thunder is an admission of a weakness (usually a mistake or failure) before that weakness is announced by another party, such as an interest group or media" (p.294).

Coombs (2012) argues that there are three basic rules when using online crisis communication channels: (1) be present, (2) be where the action is, and (3) be there for the crisis. Be present means that organization should not hide from online world. Stakeholders, including the news media, will look to the corporate web site and existing social media activities of an organization for information. If the crisis is never mentioned in the organization’s online communication, the absence will be noticeable. The organization will be criticized for being silent and miss the opportunity to present its interpretation of the crisis (p.27).

*Research question 3: Is there a significant difference between the levels of source of information (organization vs. media) considering the apologies constructed by stakeholders?*

## 3 Methodology and Research Design

To examine if there was a significant difference between the levels of type of crisis and the levels of source of information considering the apologies written by stakeholders, an experiment was conducted.

The experiment was constructed as a 2X2 between subject factorial design of independent variables (preventable vs. victim) X (media vs. organization) comparison. Based on two levels of each independent variable, four types of scenarios were created for this study. (1) Victim organizational crisis and source of information – organization; (2) preventable organizational crisis and source of information – media; (3) preventable organizational crisis and source of information – organization; and (4) victim organizational crisis and source of information – media.

### 3.1 Participant Recruitment

Participants in this study were recruited online using "SoSci Survey – the Solution for Professional Online Questionnaires."

Respondents' Profile: As a whole, more females (70%, n = 70) than males (30%, n=30) completed the survey. Most participants were 19 - 30 years (72%) and while the twenty eight percent (28% )f rom 30 – 50 years. Forty six percent (46%) of the respondents were students, forty three percent (43%) were employed full time, three percent (3%) were employed in the public sector, five percent (5 %) were self- employed, while three percent (3%) of the participants were unemployed.

After answering the demographic question, participants were asked how often do they conduct online transactions. The question was frequency scale type of question where frequencies were ordered sequentially. On this question most of participants - forty six percent (46%) replied that they conduct online transactions often. Thirty three percent (33%) of participants always conducted online transactions**,** fifteen percent (15%) - sometimes, three percent (3%) - seldom and other three percent (3%) - have never conducted online transactions before.

Participants were also asked whether their personal information including banking information has ever been stolen. Majority of participants ninety six percent (96%) have never been victims of data breach.

After consenting to be in the study, hundred (100) participants were presented with four different scenarios of data breach (twenty five participants in each scenario). Crisis type and source of information were crossed to create four basic crisis scenarios.

The first case included the scenario where the data breach was caused by hackers and the organization immediately informed the customers about the crisis. According to the second scenario, the data breach was caused by an employee who had a legitimate access to customers´ data and intentionally breached information. In this case, costumers found the information about the breach from media. In the third scenario, participants were informed about the data breach from the company itself. However, the breach was caused by an employee of this company. Finally, according to the last scenario, customers' data was stolen by hackers and the source of information was not the organization but the article on the internet.

It was interesting to examine stakeholders' perceptions of apologies in a victim as well as preventable organizational crisis. Furthermore, it was also significant to find out whether less reputational damage is inflicted when an organization notified its stakeholders about a crisis as compared to when the news media was the first to deliver such information.

As already mentioned, data breaches are ambiguous crises. On one hand, the organization is a victim of the hackers. On the other hand, the organization has failled in its responsibility to safeguard customers´ information. Accordingly, it was interesting to explore what attribution level do stakeholders regard an organization to carry when a data breach occurs by different reasons. One of the goals of this study was to identify as many different apology elements as possible and to allow different participants to assign different levels of responsibility to the organization in different types of crisis.

To explore what elements stakeholders want to see in effective organizational apology hundred participant apologies were analyzed in this study. Each of the written apologies ranged from 34 – 146 words. Data analyze began with decontextualization, first, meaning units were identified. Second stage included recontextualization - important parts of the texts were saved and less important ones were excluded. Third stage of data analysis consisted of categorization - homogenous groups in each case were identified and coded under same dimensions. The different types of apology elements were then analyzed for common themes so that they could be combined into the categories. Finally, in the selective coding step, two core categories were identified to show how all the other categories related to each other. At last, a factorial ANOVA (two – way ANOVA) was conducted to compare main effects of different types of crisis and different types of sources of information on dependent variable – apologies written by stakeholders.

# 4 Findings

In general, two dimensions - words versus behaviors, and fixing the problem versus rebuilding the relationship, were identified. In these two dimension, ten categories emerged. These dimension and categories were found in all the cases but apologies differed in quantity and content according to the type of crisis.

| | Words | Behaviors |
|---|---|---|
| Fixing Problem | • Acknowledge Responsibility<br>• Offer an explanation<br>• Tell stakeholders what actions they can take to protect themselves | • Corrective action<br>➢ Mitigate harms to stakeholders<br>➢ Offer reparations<br>➢ Prevent reoccurrence |
| Rebuilding Relationship | • Express genuine remorse<br>• Bolstering<br>• Identify with stakeholders<br>➢ Concern/empathy for individuals<br>➢ Recognize stakeholders importance/contribution<br>➢ Espouse shared values<br>• Request another chance | • Foster personal communication<br>➢ Address stakeholders appropriately<br>➢ Invite contacts<br>• Provide compensation |

**Table 2.** Types of apology elements generated by stakeholders.

The first dimension was *words versus behaviors*. all responses were in the form of words, but some words stood on their own (sharing information, expressing emotions) and some words promised behaviors (taking steps to fix the problem, offering compensation). Besides, some of the stakeholder suggestions could be conducted with words alone, but others required a company to take further steps.

The second dimension was *fixing the problem versus rebuilding the relationship*.
Some apology elements were aimed at preventing, minimizing, or repairing damage caused by the crisis. Other apology elements and suggestions did not solve the immediate problem, but tried to show concern for stakeholders and reestablish trust. Accordingly, apology elements written by stakeholders can be classified as either (1a) words to fix the problem, (1b) behaviors to fix the problem, (2a) words to rebuild the relationship, or (2b) behaviors to rebuild the relationship

### *Words to Fix the Problem*

When an organization apologizes for a crisis, stakeholders expect the organization to fix the problem. This process involves words and behaviors. Most of the written apologies in all the cases included at least one example of words being used to fix the problem. However, there was difference considering the type of crisis.

The data suggested that organizations could use words to fix problems by acknowledging responsibility, offering an explanation, and telling stakeholders what actions to take.

#### *Acknowledging responsibility*

Coombs (2015) argued that “full apologies must acknowledge the crisis, accept responsibility, include a promise not to repeat the crisis, and express concern and regret” (p. 148). When companies announces statements of sympathy or regret without accepting responsibility, these are non-apologies, although stakeholders “often accept these non-apologies as true apologies” (p. 148). As Lee and Chung (2012) found there is also difference between active and passive responsibility. Stakeholders respond more negatively to the passive responsibility, as it can be perceived as defensive and morally unacceptable (p.932-934).

As well as Shuman (2000) said, apologies can be effective only when the organization acknowledges its responsibility and takes favorablee steps to repair the damage if the fault is clear. On the contrary, a passive responsible apology has less chance to resolve disputes in which the extent of each party's fault is clear.

Participants of this survey indicated a desire companies to acknowledge responsibility directly. It is worth mentioning that in the scenario where the breach was caused by the employee, more participants required from the organization to acknowledge responsibility for the damages caused, in comparison to the scenarios where breach was caused by a hacker. Twelve percent (12 %) of participants in the first scenario wanted organization to acknowledge its' responsibility for the occurred crisis. Forty percent (40%) of participants expressed the same desire in the second scenario. This was the case in thirty two percent (32%) of apologies in the third scenario, and twenty percent (20%) in the fourth scenario. For instance, one of the apologies contained a statement: "We would like to assure you that we take full responsibility for the inconvenience created and will do whatever is necessary to win your trust back." One participant also wrote: "It is our responsibility to store customer data securely so that no third party can gain knowledge of it. Unfortunately, this time we did not succeed and for this we would like to apologize sincerely." Another apology included the following statement: "Please accept our sincere apologies for all the inconvenience caused, we take the whole responsibility for the above-mentioned events.'' It is clear from these examples that the importance of acknowledging the responsibility is extremely significant for stakeholders. Furthermore, they look for active responsibility as an apology from organizations.

### *Offer explanation*

According to Coombs (2012): "On a basic level, stakeholders need to know what happened: what, when, where, why, and how of the crisis" (p.148). The openess of an organization is a multidimensional concept. Openness means willingness to disclose information and honesty. In a crisis, the focus is on media, but stakeholders may ask or demand that their questions be answered. During a crisis, normally the responsibility is taken by a spokespersons or other crisis team members who try to make every reasonable attempt to respond to questions promptly (p.144).

Participants in all of the cases expressed the desire an organization to offer a brief explanation about the crisis. The number of apologies which included desire for more explanation from the organization differs related to the source of information about the occurred crisis, which is statistically proved and presented in the next chapter. More participants asked for brief explanation about occurred crisis in those cases where the source of information was media and not the organization directly. Twelve percent (12%) of stakeholders in the first scenario expressed willingness organizations to offer them explanation about the occurred crisis. Thirty six percent percent (36%) of stakeholders in the second scenario asked for explanation about occurred crisis. Twenty - four percent (24%) - in the third scenario. The same desire was evident in thirty two percent (32%) of apologies written by stakeholders in the fourth scenario. For instance, participants who were informed about the breach from media and not directly from the organization, wrote the following statement: "We are sincerely sorry for what has happened. On behalf of my team I wanted to reach out to you personally (!) and offer you - if you so wish - insight in some of the things that have happened". One of apologies also included: "We kindly want to inform you that your personal data (including name, e-mail and postal address) might have been stolen by that person.''

### *Telling stakeholders what actions to take*

Telling stakeholders what they can do to protect themselves is another way of using words to fix the problem. Instructing information focuses on telling the stakeholders what to do to protect themselves in the crisis. People are the priority in any crisis, so instructing information must come first. In the Crisis phase, stakeholders need to know how the crisis will or might affect them. They should be told if there is anything they need to do to protect themselves. Instructing information satisfies the needs of stakeholders and as well as of the crisis teams`. The stakeholders receive the information they require to protect themselves. This helps crisis team to be perceived as capable of handling the situation properly (Coombs, 2012; p.146).

This was the case in sixteen percent (16% ) in the first scenario, thirty two percent (32%) in the second scenario, twenty eight percent (28%) in the third scenario, and twenty four percent (24%) in the fourth scenario. Most of participants of those scenarios where breach was caused by an employee demanded organizations to guarantee them that their personal information would not be further used for any illegal activities. On the other hand, in those cases where the crisis occurred by an intervention of hackers, the majority of the participants expressed desire to be explained detailly what steps should be taken after the crisis. As an example, one of the respondents wrote: "We have to ask you to contact your bank representative and take the measures if you had any transactions on our website during the last 5 days. Our advice is to block and renew the card." Other participants wrote: "In case you are a victim of the incident please, contact legal forces and our help center for cooperation.''

### *Behaviors to Fix the Problem*

Part of the job of an organizational apology is to communicate what behaviors the organization is engaged in to fix the problem. These behaviors are described in the promises of forbearance, offers of repair, and efforts to mitigate harm.

### *Promises of Forbearance*

Almost the same number of participants of all the cases wrote about preventing a reoccurrence of the problem. Thirty six percent (36%) of apologies in the first scenario expressed willingness the crisis not to reoccur again. Fifty six percent (56%) of apologies expressed the same desire in the second scenario. Forty eight percent (48%) of stakeholders in the third cenario wrote about their wish crisis not to occur anymore. Thirty two percent (32%) expressed the same desire in the fourth scenario. Although, many participants in all four scenarios required the company to prevent reoccurrence of the breach, the cause of the breach still played a vital role when it came to promising the non-reoccurance of the crisis. One suggestion read: "We assure you this will not happen again and your information is safe with us for future transactions." As another example, one of the statements included: "Be sure that we are working actively on eradicating this issue from happening in the future, as well as stopping your personal information to further be used for any illegal activities.''

### *Offers of Repair*

Approximately half of the participants in the second scenario (48%) mentioned compensating the loss or receiving a gift form an organization. An apology from the second scenario stated: “In case of any damage to your banking information/account, our company will compensate everything.” Another statement in the same scenario included: “I would like to compensate the inconvenience by providing you our loyalty card which was created by our team for this particular event.’’

### *Mitigating Harm*

Another type of corrective action is the mitigation of harm. This element was evident in sixteen percent (16 %) of responses in the first scenario, in fifty two percent (52%) of responses in the second scenario, in forty eight (48%) of responses in the third scenario, and in  twenty four (24%) of responses in the fourth scenario. For instance, in those scenarios where the hacker committed a crime, some statements included the following content: “Please understand that our team is doing everything to find out the sources of this illegal activity. We will absolutely re-update our security system to make sure this never happens again.” In those cases where the breach was caused by an employee, one of the respondents wrote the following: “We want to make clear that it was only one of our employees who is no longer working here and will have to face legal consequences.”

These behaviors do not constitute reparations, nor do they ensure the problem will never reoccur. However, they do help to reduce the damage caused in immediate future, and apparently, they contribute to the effectiveness of an apology.

### *Words to Rebuild the Relationship*

According to Bentley (2018): “Just because an organization fixes a problem does not mean it automatically regains legitimacy in the eyes of its stakeholders” (P.218). Stakeholders in all the scenarios identified three ways organizational apologies can use words to rebuild stakeholder relationships. Apologies can express genuine remorse, identify with stakeholders, and ask victims for a second chance.

*Express Genuine Remorse*

Almost all apologies contained either the word "apologize" or the word "sorry." More interesting is the number of participants who used adverbs such as "sincerely," "deeply," or "truly," or "really," "extremely," "incredibly," "from the bottom of our heart" to intensify the apology.

Expression of genuine remorse was evident in forty percent (40%) of apologies written in the first scenario, sixty percent (60%) in the second scenario, forty four percent (44%) in the third scenario, and eight percent (8%) in the fourth scenario.

One participant in the third scenario wrote: "If you can apologize to customers effectively, you can turn around a bad situation. However, if you can't apologize genuinely, your customers will be left to assume that you just don't care." Another participant in the first scenario wrote: "We are really sorry and apologize from the bottom of our heart for the inconvenience this situation brings for you.''

*Identification with Stakeholders*

According to Burke (1969): "Identification occurs when the goals, values, or interests of two parties align." As Cheney (1983) explained, organizations often use communication to make members feel that the organization shares their interests. Common techniques for fostering identification between organizations and members include "Expression of concern for the individual" (p. 150), "Recognition of individual contributions" (p. 150), and "Espousal of shared values" (p. 151). The present data suggests that similar techniques may be appropriate in organizational apologies.

- Express concern/empathy for individuals - For example, concern for individuals was expressed in empathetic statements like: "We realize how frustrating this situation might be for you'' or "we undoubtedly understand your concern about the breach.'' Concern/empathy appeared in eight percent (8%) in responses of the first scenario, in fifty six percent (56%) in responses of the second scenario, in forty four percent (44%) in the responses of the third scenario, and sixteen percent (16%) in the fourth scenario.

- Recognition of individual contributions - the contribution of individual customers was recognized in statements such as: "You as a client are very valuable to us," ''the protection of data is of utmost importance in our company." In the second scenario where the crisis was caused by the organization and source of information was media, the highest number of participants (52%) required the organization to mention how important the customers are for them. For example, one participant wrote: "We value our customers to the fullest and your satisfaction is our priority."

- Espouse shared values - Espousal od shared values was evident in statements like - "we hope to show you that transparency is still at the top of our goals." Another statement included: "The security of your data is the most important for our company. As well as transpareny and communication with our clients in top of our interests. " It is worth mentioning that especially those participants who learned about the crisis from media expected organizations to hold the same values, for example "transparency." The statements of participants of the second scenario expressed willingness to espouse shared values most frequently (52%). Only twelve percent (12 %) of participants expressed the same willingness in the first scenario.

*Bolstering*

Bolstering suggests reminding people of the good things the organization had done. Sheldon and Sallot (2009) reported that apologies were more effective than bolstering (i.e., highlighting one's good points) or corrective action (i.e., repairing damage) in restoring a politician's reputation after a faux pas. By contrast, Coombs and Schmidt (2000) found no significant differences between apologies, corrective action, bolstering, or shifting blame when they tested college students' reactions to an organization's crisis communication.

It is worth mentioning that the second scenario included highest number of responses including this element (28%) as well as third scenario (24%). For example, one apology said: "Our company is committed to high standard. We always strive to provide you with the best possible service and truly value your business."

### *Request Another Chance*

A desire of participants organizations to ask for another chance to cooperate with them was evident in twenty four percent (24%) of statements in the second scenario, in four percent (4%) in the first scenario, in sixteen percent (16%) in the third scenario and finally it was evident in twelve percent (12%) - in the fourth scenario. For example, one apology included: "I hope that you will give us the opportunity to earn back your trust and confidence in future seasons."

### *Behaviors to Rebuild Relationships*

Organizations can also use apologies to describe certain *behaviors* that may help rebuild relationships with stakeholders. The data from all four cases indicate that organizations should consider providing compensation and fostering personal communication with stakeholders.

### *Providing compensation*

Providing compensation to crisis victims is not the same as offering a repair. As Benoit (1995) explained, an offer of repair, or corrective action, "addresses the actual source of injury" while compensation is "a gift designed to counterbalance, rather than to correct, the injury" (p.79). One of the most frequently used mentioned desire was providing compensation which was evident in thirty six percent (36%) of written apologies in the first scenario, in fifty six percent (56 %) in the second scenario, in forty six percent (46%) in the third scenario and in thirty two percent (32%) in the fourth scenario. For example, one of the apologies said following: “We are committed to compensate any possible damage to our clients.” For some people at least, compensation is a symbolic apology: “We also would like to give you a gift card of 100$ for the damage we've caused.” Another apology included: “We are committed to compensate any possible damage to our clients.”

## Fostering Personal Communication

Along with compensating victims, other behaviors can help rebuild relationships between organizations and stakeholders. These behaviors are related to fostering personal communication. Some of participants expect organization to express its’ readiness to communicate with the stakeholders whenever they want and inform them in more detail about occurred crisis and further steps. Some participants also indicated that they wanted to be addressed by name.

It is worth mentioning that the number of apologies according to which participants expect organizations to foster personal communication with them is obviously higher in those two scenarios where the stakeholders were informed about the breach from media, which is confirmed statistically in the next chapter. In the second scenario where the source of information about the breach was media forty six percent (46%) of participants indicated they want organizations to express the readiness to communicate with them whenever they wanted. The same desire was evident in forty four percent (44%) of participants in the fourth scenario where the source of information about the breach was also media. For example, one apology included: “If you like to gain more information, don't hesitate to contact us.” One of the participants also wrote: “If you have any questions or want to talk about it please don't hesitate to either call or e-Mail us.’’

|  |  |  |  |  |
|---|---|---|---|---|
| Theme | ▪ Data breach caused by hacker<br>▪ Source of information – organization (First scenario) | % | ▪ Data breach caused by employee<br>▪ Source of information - media<br>(Second scenario) | % |
|  | example |  | example |  |
| Acknowledge responsibility | ▪ We are sincerely sorry for the damages we have cost you<br>• It is our responsibility to store customer data securely so that no third party can gain knowledge of it. Unfortunately, this time we did not succeed and for this we would like to apologize sincerely. | 12 | • Our company takes responsibility for the error, and we are committed to compensate any possible damage to our clients. | 40 |
| Offer Explanation | • If you are interested in a personal talk about this situation, please do not hesitate to contact us.<br>• We kindly want to inform you that your personal data (including name, e-mail and postal address) might have been stolen by that person. | 12 | • We are sincerely sorry for what has happened. On behalf of my team I wanted to reach out to you personally (!) and offer you - if you so wish- insight in some of the things that have happened<br>• If you have any questions or want to talk about it please don't hesitate to either call or e-Mail us<br>• A comprehensive apology explaining the whole situation in detail. | 36 |

| | | | | |
|---|---|---|---|---|
| | | | | |
| Correcting action Mitigate harm | • Please understand that our team is doing everything to find out the sources of this illegal activity. We will absolutely re-update our security system to make sure this never happens again. | 16 | • We have invested in a new system, that works like a cyber intelligence and will back check everything going on, so that something like this will never happen again<br>• The Bank is working extensively to insure that the leaked information has been secured and changed in time.<br>• We want to make clear that it was only one of our employees who is no longer working here and will have to face legal consequences | 32 |
| Offer reparations | • To apologize, we offer you a coupon or X amount of money to be spent on our website.<br>• Please accept an apology gift | 16 | • As an apology, please accept this small gift from us (credit for the shop)<br>• We know money can't make up for the breach of trust but we want to give you this 50€ voucher to express our apologies. | 52 |

| | | | | |
|---|---|---|---|---|
| | from us chosen according to your taste | | • Also you can use our gift voucher with it you can shop online with 50% off.<br>• In case of any damage to your banking information/account, our company will compensate everything | |
| Prevent reoccurrence | • We will absolutely re-update our security system to make sure this never happens again.<br>• We assure you this will not happen again and your information is safe with us for future transactions<br>• Our team is working 24/7 to strengthen the cyber security of the platform | 20 | • Be sure that we are working actively on eradicating this issue from happening in the future<br>• At the same time we are working on improving our systems and structures to prevent such situations in the future in the best possible way.<br>• A new system will be implemented to never make this happen again. | 48 |

Table 3. Examples and Frequencies of Problem Fixing Themes

| Theme | Data breach caused by employee<br><br>Source of information - organization<br><br>(Third scenario) | Number of Participants | Data breach caused by hacker<br><br>Source of information – media<br><br>(Fourth scenario) | Number of Participants |
|---|---|---|---|---|
| | example | | example | |
| Acknowledge responsibility | • we would like to assure you that we take full responsibility for the inconvenience created and will do whatever is necessary to win your trust back.<br>• we thoroughly take that responsibility and will do our best to find out the hackers | 32 | • In this instance, we did not live up to our own standard, and for that we offer a most sincere apology.<br>• we apologize for the inconvenience and as the problem was caused by our own security flaw | 20 |
| Offer Explanation | • Due to the fact that it is important for us to cooperate with you, we have decided to warn you about this cyber attack<br>• Due to that fact, we decided to warn you about it, because we do care and appreciate with cooperation with our clients | 24 | • Sorry that you heard about the news through an article instead of us getting in touch with you before that<br>• Should you have any questions or if I can be of any further assistance, please do not hesitate to contact me<br>• It is a company's responsibility to inform be about such incident. | 32 |

| | | | | |
|---|---|---|---|---|
| | | | Such neglecting and hiding the fact of breach is unprofessional from the side of the company | |
| Correcting action<br>Mitigate harm | • Our team is working very hard to resolve the issue and find out the exact extent of the problem.<br>• will do the best to make sure that he/she will get arrested<br>• we will assess the situation and deliver the solution<br>• Consider improving your account security by implementing 2 factor authentication so this leak would not have big impact on you<br>• As soon as we discovered the problem we have started to investigate the following incident. | 48 | • We want to reassure you that the security gap has been fixed and no further data can be stolen.<br>• let me assure you that it will not have any consequences on your business and daily life<br>• We will do everything in our power to stop them from further invading our and most importantly your privacy.<br>• Unfortunately we are still resolving the issue of your personal information being leaked online, thus we ask you to be patient while the matter is being resolved. | 24 |
| Offer reparations | • We would like to express our sincere apology to you and give you several benefits from our | 28 | • I would only be completely satisfied with the companies' apology I think if they offer | 24 |

| | | | | |
|---|---|---|---|---|
| | company such as becoming our VIP client.<br>• transfer money back<br>• In case you still decide to stay with us, u will be honored as our very special client and be provided with various of additional services for free.<br>• I'll be glad if I was refunded and still got the item that I ordered as a compensation for the following situation. | | some compensation, discount code, etc.<br>• Please accept this (20% of whatever was stolen) gift card from us.<br>• As soon as we restart our website, you'll get the email and -50% promo code on our website.<br>• As a sign of your appreciation we present you with $ 50 gift card. | |
| Prevent reoccurrence | • we will do our best to strengthen our cyber security<br>• Of course we will make sure that this will never happen again in the future.<br>• We are thoroughly working to improve our security standards for this kind of situations to never happen again | 48 | • In order to assure you that the incident does not repeat itself we have taken the necessary security measures to protect as many accounts as possible.<br>• We are doing everything we can to make sure such an occurrence becomes impossible, and hope you have not lost your trust in us as a company | 32 |

| | | | | |
|---|---|---|---|---|
| | | | - We will do everything in our power to stop them from further invading our and most importantly your privacy. | |

Table 4. Examples and Frequencies of Problem Fixing Themes

| | | Answers including specific themes in % | | | |
|---|---|---|---|---|---|
| Theme | Example | Type of crisis – victim, Source – organization<br>(First scenario) | Type of crisis – preventable, Source – media<br>(Second scenario) | Type of crisis – preventable, Source – organization<br>(Third scenario) | Type of crisis – victim Source - media<br>(Fourth scenario) |
| 1. Express genuine remorse | We would like to offer our sincere Apology.<br>We are really sorry and apologize from the bottom of our heart. | 36 | 84 | 60 | 24 |
| 2. Identify with stakeholders<br>- Express concern/empathy for individuals | We realize how frustrating this situation might be for you.<br>We undoubtedly understand your concern | 8 | 56 | 44 | 16 |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  | about the breach. |  |  |  |  |
| • Recognize stakeholders' importance | You as a client are very valuable to us. The protection of data is of utmost importance in our company. | 12 | 52 | 44 | 12 |
| • Espouse shared values | We hope to show you that transparency is still at the top of our goals. | 12 | 52 | 46 | 16 |
|  | Company's main priority is to gain our customers' trust. Unfortunately, in 21st century we are vulnerable towards cyber- attacks and are well aware of their consequences. |  |  |  |  |
| 3.Request another chance | I hope that you will give us the opportunity to earn back your trust and confidence in future seasons. | 4 | 24 | 16 | 12 |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| 4.Provide compensation | We are committed to compensate any possible damage to our clients.<br>We also would like to give you a gift card of 100$ for the damage we've caused. | 36 | 56 | 46 | 32 |
| 5. Foster personal communication<br>• Invite stakeholders to contact organization<br>• Address stakeholder appropriately | If you like to gain more information, don't hesitate to contact us. | 20 | 46 | 36 | 44 |
|  | Dear X (I would start with a name of the customer, to make more personal) | 12 | 56 | 52 | 16 |
| 6. Bolstering | We as a rapidly growing business, relying primarily on user experience try to evolve around the theme of personalized content, therefore we | 4 | 28 | 24 | 8 |

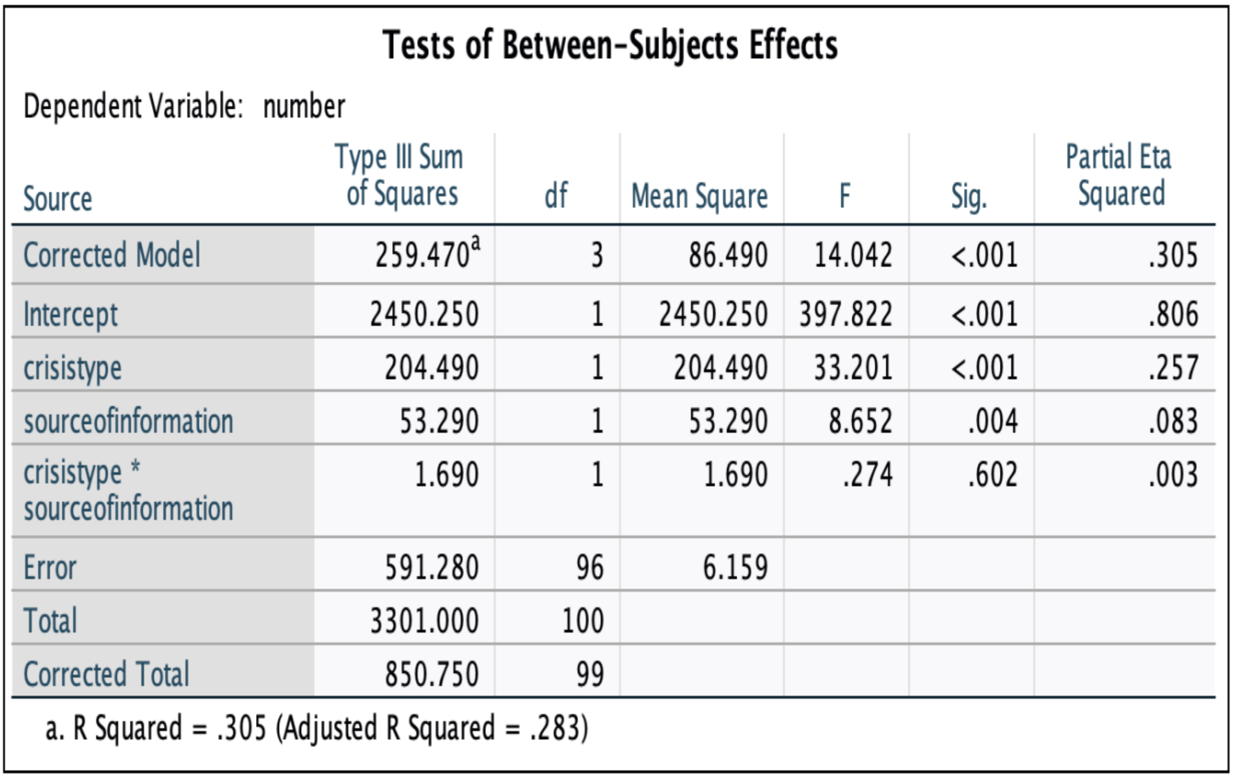
| | | | | | |
|---|---|---|---|---|---|
| | have multitude of employees who research the preferences and tastes of different individuals. We had assumed that serving to a good cause would | | | | |

Table 5. Examples and Frequencies of Relationship Rebuilding Themes.

### *4.1 Factorial Anaysis*

As already mentioned, a factorial ANOVA (two – way ANOVA) was conducted to compare main effects of different types of crisis and different types of  sources of information on the dependent variable – apologies written by stakeholders.

As expected, crisis type and in some cases  - source of information had influence on how stakeholders constructed apologies. The results showed that there was a significant difference between the levels of crisis type (preventable vs. victim) and source of information (organization vs. media) on the dependent variables – apologies written by stakeholders.



**Tests of Between-Subjects Effects**

Dependent Variable: number

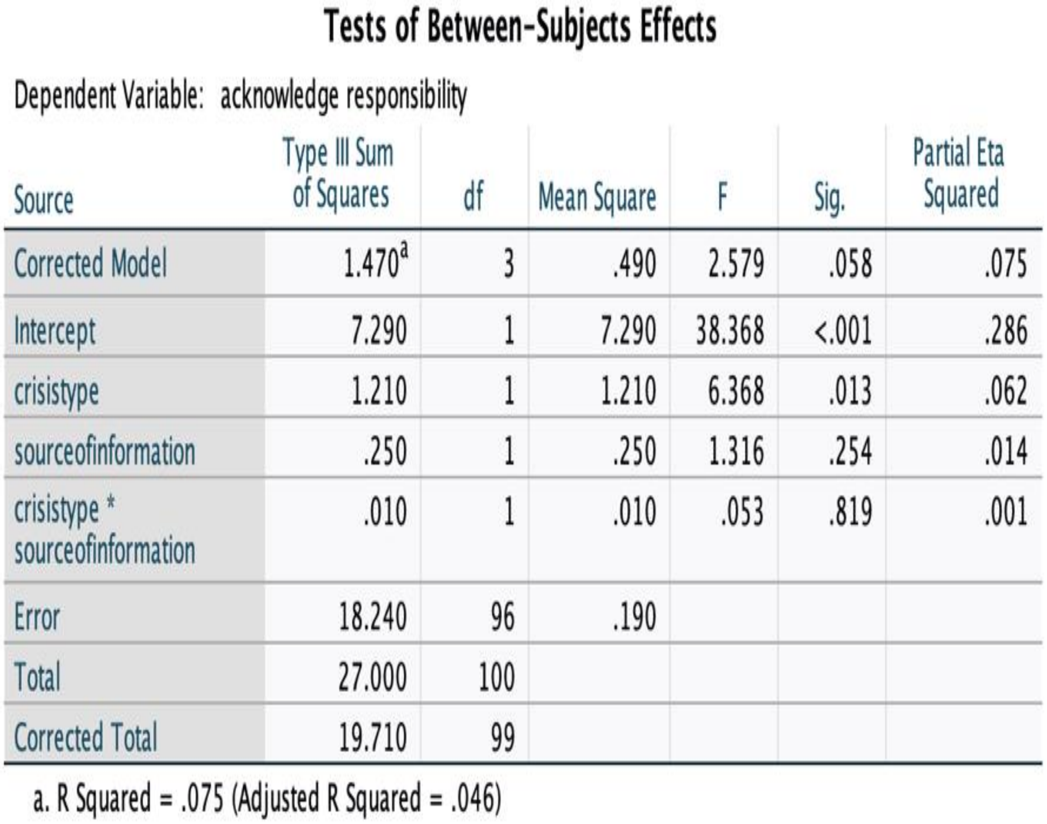
| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 259.470a | 3 | 86.490 | 14.042 | <.001 | .305 |
| Intercept | 2450.250 | 1 | 2450.250 | 397.822 | <.001 | .806 |
| crisistype | 204.490 | 1 | 204.490 | 33.201 | <.001 | .257 |
| sourceofinformation | 53.290 | 1 | 53.290 | 8.652 | .004 | .083 |
| crisistype * sourceofinformation | 1.690 | 1 | 1.690 | .274 | .602 | .003 |
| Error | 591.280 | 96 | 6.159 | | | |
| Total | 3301.000 | 100 | | | | |
| Corrected Total | 850.750 | 99 | | | | |

a. R Squared = .305 (Adjusted R Squared = .283)

Table 5. tests of between – subjects effects on the number of apologies

Type of crisis (P<001) and source of information (P=004) we statistically significant. Which indicates that there was significant difference between the levels of both independent variables on dependent variable – number of apologies constructed by stakeholders. The main effect of crisis type yielded an effect size of 25,7, indicating that 25,7% of variance in number of apologies was explained by crisis type (F (1,96) = 33.201, P<.001). The main effect of source of information yielded an effect size of 0.083, indicating that 8,3% of variance in number of apologies was explained by source of information (F(1, 96)=8.652, P=.004).

It was also interesting to examine whether there was a significant difference between the levels of each independent variable separately considering all types of apologies constructed by stakeholders.



Tests of Between-Subjects Effects

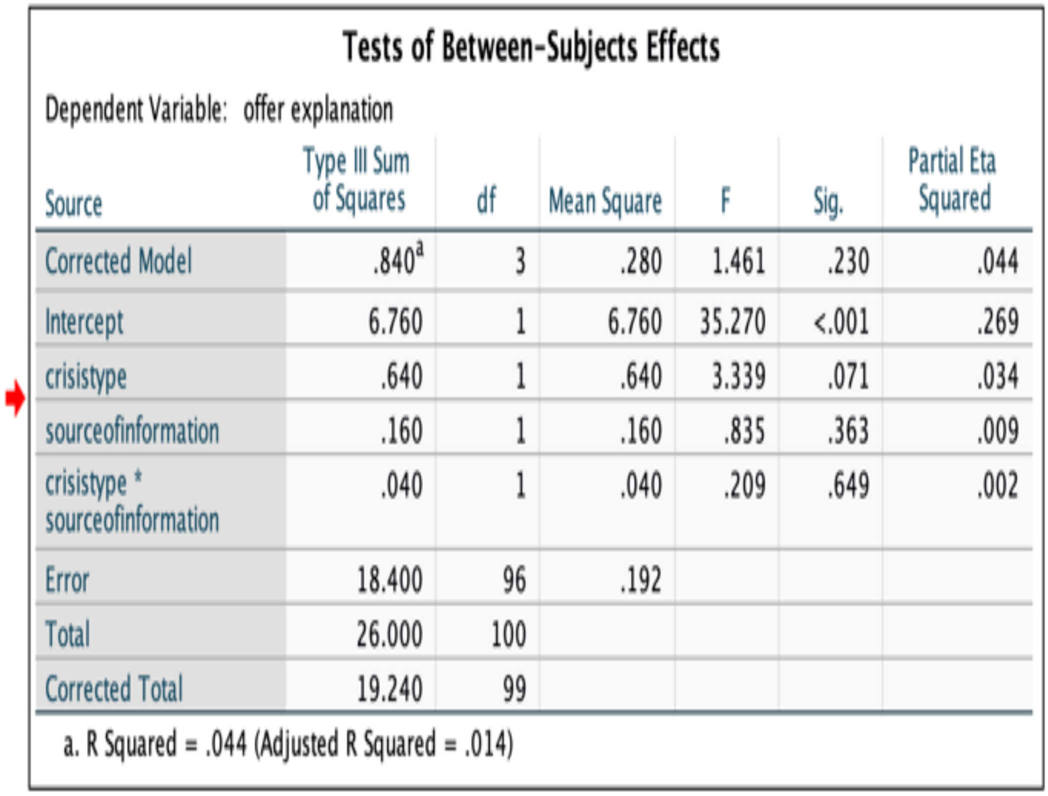
Dependent Variable: acknowledge responsibility

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 1.470[a] | 3 | .490 | 2.579 | .058 | .075 |
| Intercept | 7.290 | 1 | 7.290 | 38.368 | <.001 | .286 |
| crisistype | 1.210 | 1 | 1.210 | 6.368 | .013 | .062 |
| sourceofinformation | .250 | 1 | .250 | 1.316 | .254 | .014 |
| crisistype * sourceofinformation | .010 | 1 | .010 | .053 | .819 | .001 |
| Error | 18.240 | 96 | .190 | | | |
| Total | 27.000 | 100 | | | | |
| Corrected Total | 19.710 | 99 | | | | |

a. R Squared = .075 (Adjusted R Squared = .046)

Table 6. tests of between – subject effects on dependent variable - acknowledge responsibility

Type of crisis was statistically significant P= .013 Which indicates that there was a significant difference between victim and preventable organizational crisis on acknowledging of responsibility by stakeholders. The main effect of crisis type yielded an effect size of 0.062, indicating that 6,2% of variance in number of apologies was explained by crisis type (F(1, 96)=6.368, P=0.02). However, source of information was not significant P=.254, which means that there was no significant difference between source of information - whether stakeholders were informed about crisis from media or organization.



**Tests of Between-Subjects Effects**

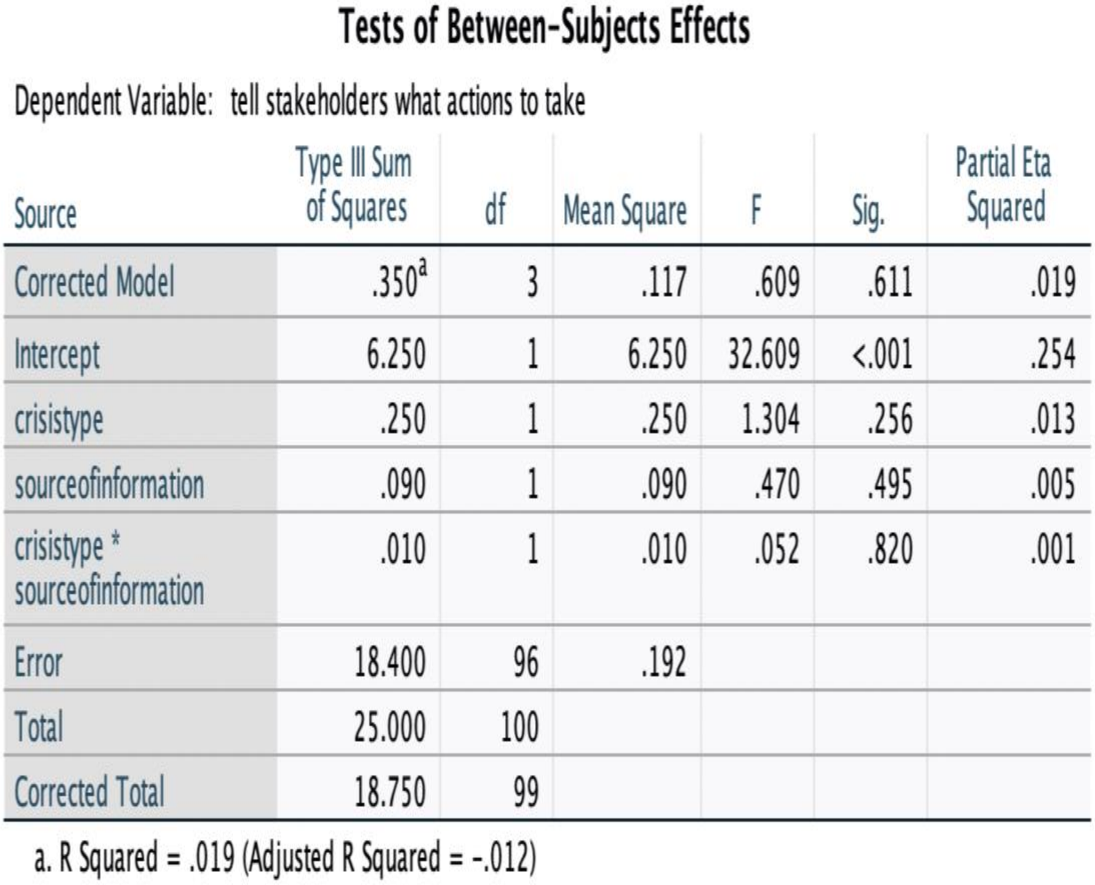
Dependent Variable: offer explanation

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | .840[a] | 3 | .280 | 1.461 | .230 | .044 |
| Intercept | 6.760 | 1 | 6.760 | 35.270 | <.001 | .269 |
| crisistype | .640 | 1 | .640 | 3.339 | .071 | .034 |
| sourceofinformation | .160 | 1 | .160 | .835 | .363 | .009 |
| crisistype * sourceofinformation | .040 | 1 | .040 | .209 | .649 | .002 |
| Error | 18.400 | 96 | .192 | | | |
| Total | 26.000 | 100 | | | | |
| Corrected Total | 19.240 | 99 | | | | |

a. R Squared = .044 (Adjusted R Squared = .014)

Table 7. tests of between – subject effects on dependent variable – offer explanation

There was no significant difference neither between the levels of crisis type (P = .071) nor in the levels of source of information (P=.363) on the dependent variable - offering explanation.



Tests of Between-Subjects Effects

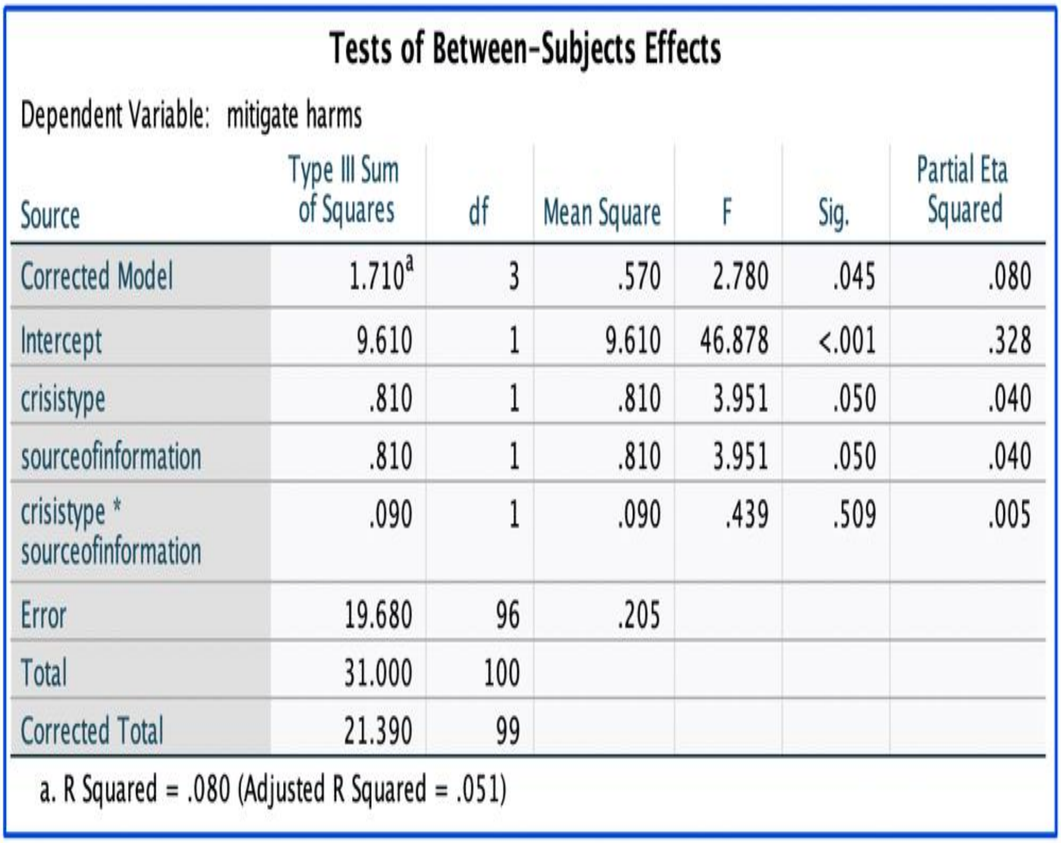
Dependent Variable: tell stakeholders what actions to take

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | .350[a] | 3 | .117 | .609 | .611 | .019 |
| Intercept | 6.250 | 1 | 6.250 | 32.609 | <.001 | .254 |
| crisistype | .250 | 1 | .250 | 1.304 | .256 | .013 |
| sourceofinformation | .090 | 1 | .090 | .470 | .495 | .005 |
| crisistype * sourceofinformation | .010 | 1 | .010 | .052 | .820 | .001 |
| Error | 18.400 | 96 | .192 | | | |
| Total | 25.000 | 100 | | | | |
| Corrected Total | 18.750 | 99 | | | | |

a. R Squared = .019 (Adjusted R Squared = -.012)

Table 8. tests of between – subject effects on dependent variable – offer expalanation

There was no significant difference between the levels of crisis type and source of information. Accordingly, neither source of information nor crisis type played vital role when it came to telling stakeholders what actions to take after the breach.



**Tests of Between-Subjects Effects**

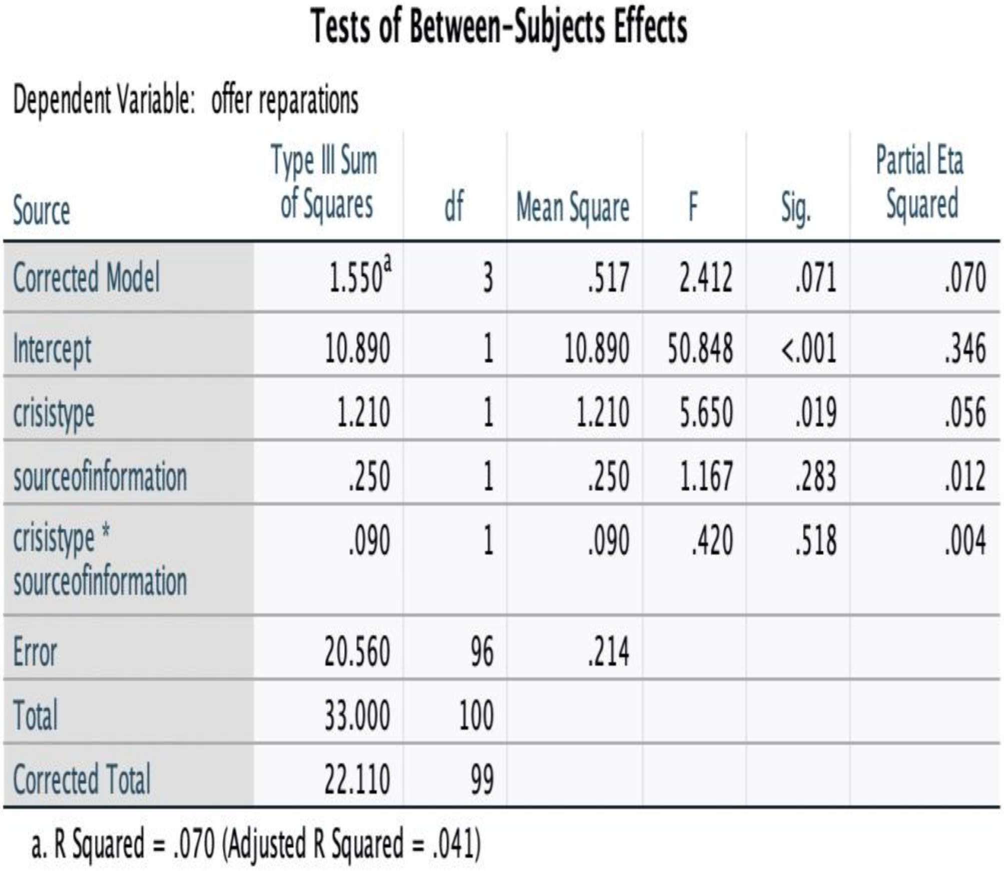
Dependent Variable: mitigate harms

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 1.710[a] | 3 | .570 | 2.780 | .045 | .080 |
| Intercept | 9.610 | 1 | 9.610 | 46.878 | <.001 | .328 |
| crisistype | .810 | 1 | .810 | 3.951 | .050 | .040 |
| sourceofinformation | .810 | 1 | .810 | 3.951 | .050 | .040 |
| crisistype * sourceofinformation | .090 | 1 | .090 | .439 | .509 | .005 |
| Error | 19.680 | 96 | .205 | | | |
| Total | 31.000 | 100 | | | | |
| Corrected Total | 21.390 | 99 | | | | |

a. R Squared = .080 (Adjusted R Squared = .051)

Table 8. tests of between – subject effects on dependent variable – mitigating harms

The results in Table 8 indicate that there was a significant difference between a victim and preventable organizational crisis (P=.05) as well as levels of source of information (P=.050) on the dependent variable - mitigating harms. The main effect of crisis type yielded an effect size of 0.040, indicating that 4% of variance in number of apologies was explained by crisis type (F (1, 96) =3.951, P=0.05). There was also significant difference between the levels of source or information – when stakeholders were informed about crisis from media or organization, (F (1, 96) =3.951, P=0.05).



Tests of Between-Subjects Effects

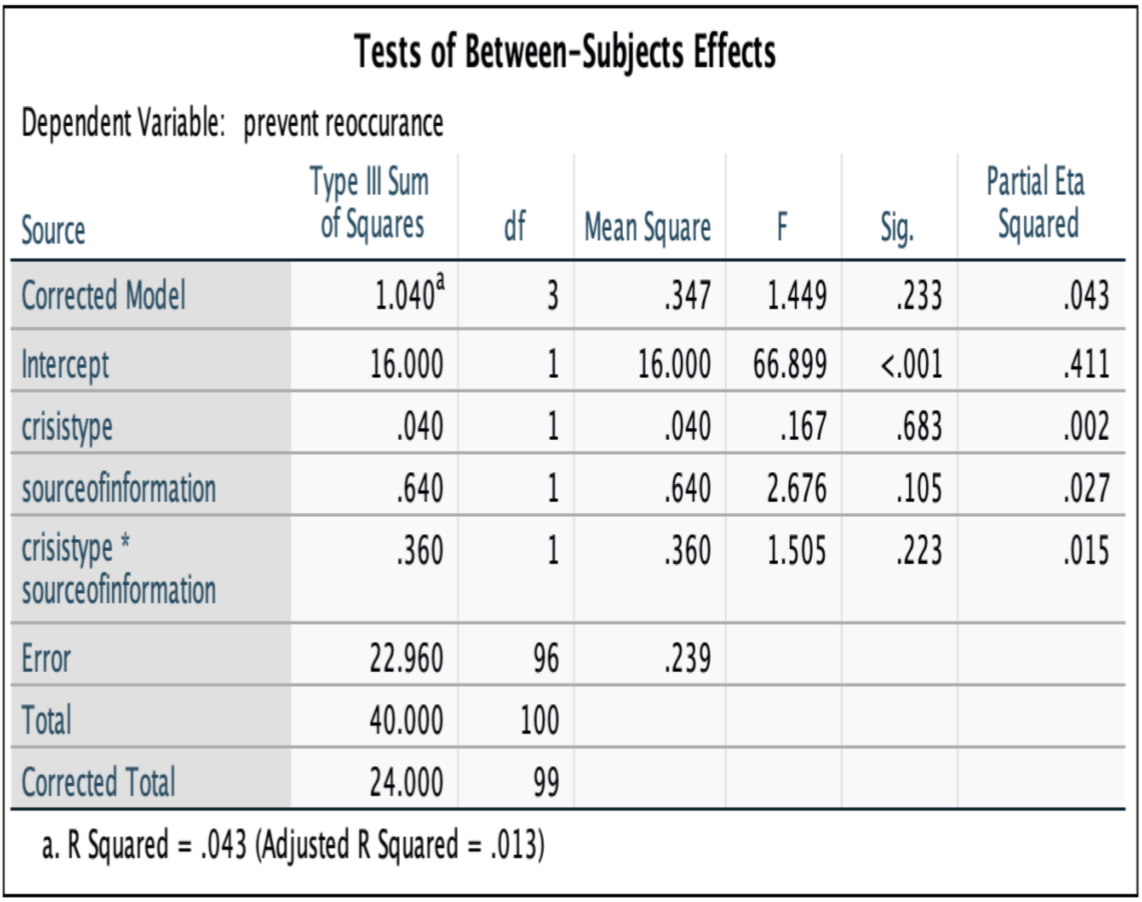
Dependent Variable: offer reparations

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 1.550[a] | 3 | .517 | 2.412 | .071 | .070 |
| Intercept | 10.890 | 1 | 10.890 | 50.848 | <.001 | .346 |
| crisistype | 1.210 | 1 | 1.210 | 5.650 | .019 | .056 |
| sourceofinformation | .250 | 1 | .250 | 1.167 | .283 | .012 |
| crisistype * sourceofinformation | .090 | 1 | .090 | .420 | .518 | .004 |
| Error | 20.560 | 96 | .214 | | | |
| Total | 33.000 | 100 | | | | |
| Corrected Total | 22.110 | 99 | | | | |

a. R Squared = .070 (Adjusted R Squared = .041)

Table 10. tests of between – subject effects on dependent variable – offer reparations

There was a significant difference between preventable and a victim organizational crisis on the dependent variable - offering reparations (F (1, 96) =1.210, P=0.02). However, there was no significant difference between levels of source of information, which means that stakeholders required from organization to offer them reparations caused by the breach without considering whether they heard about the breach from media or the organization.



**Tests of Between-Subjects Effects**

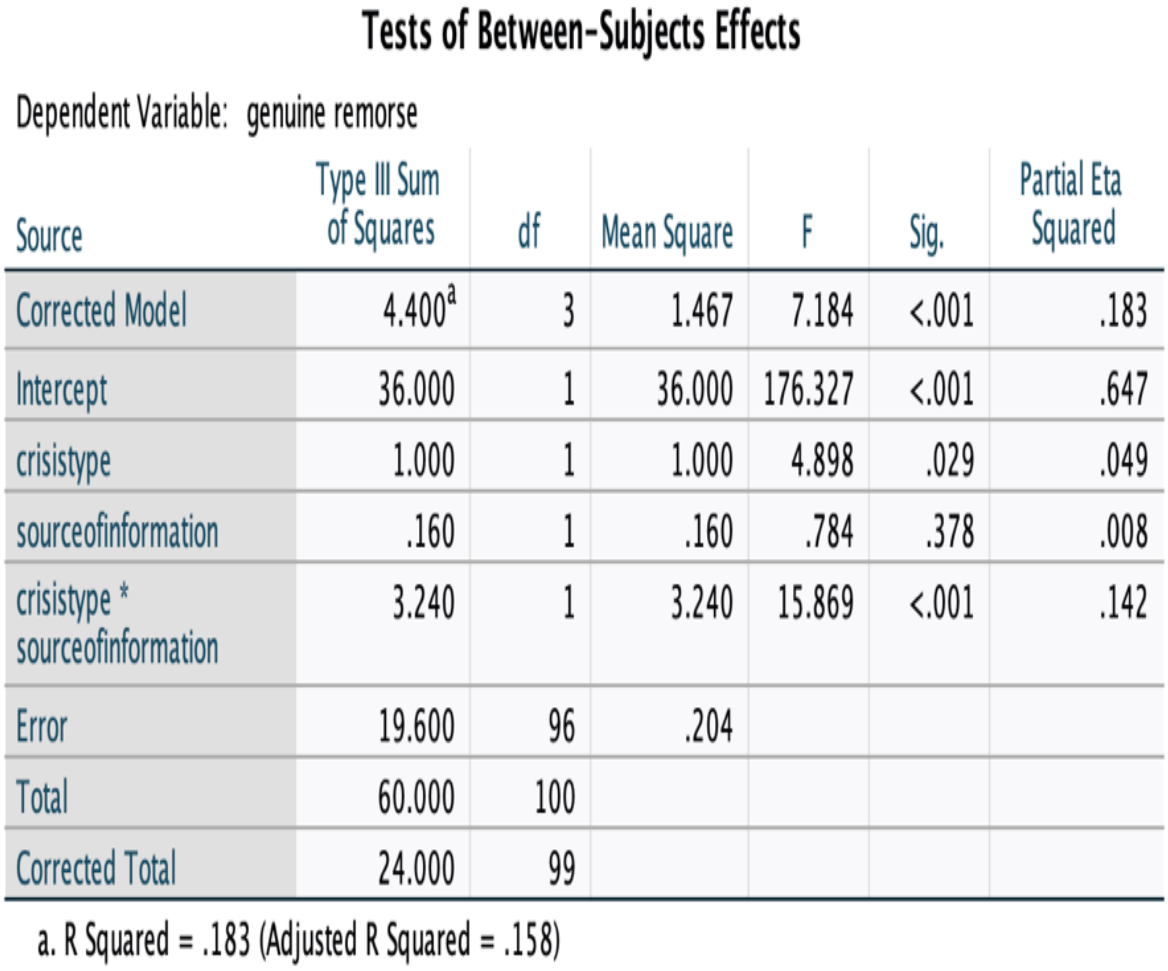
Dependent Variable: prevent reoccurance

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 1.040[a] | 3 | .347 | 1.449 | .233 | .043 |
| Intercept | 16.000 | 1 | 16.000 | 66.899 | <.001 | .411 |
| crisistype | .040 | 1 | .040 | .167 | .683 | .002 |
| sourceofinformation | .640 | 1 | .640 | 2.676 | .105 | .027 |
| crisistype * sourceofinformation | .360 | 1 | .360 | 1.505 | .223 | .015 |
| Error | 22.960 | 96 | .239 | | | |
| Total | 40.000 | 100 | | | | |
| Corrected Total | 24.000 | 99 | | | | |

a. R Squared = .043 (Adjusted R Squared = .013)

Table 11. tests of between – subject effects on dependent variable – prevent reoccurance

Regarding the preventing reoccurrence, neither crisis type, nor source of information played important role. There was no significant difference between the levels of crisis type and the levels source of information.



Tests of Between-Subjects Effects

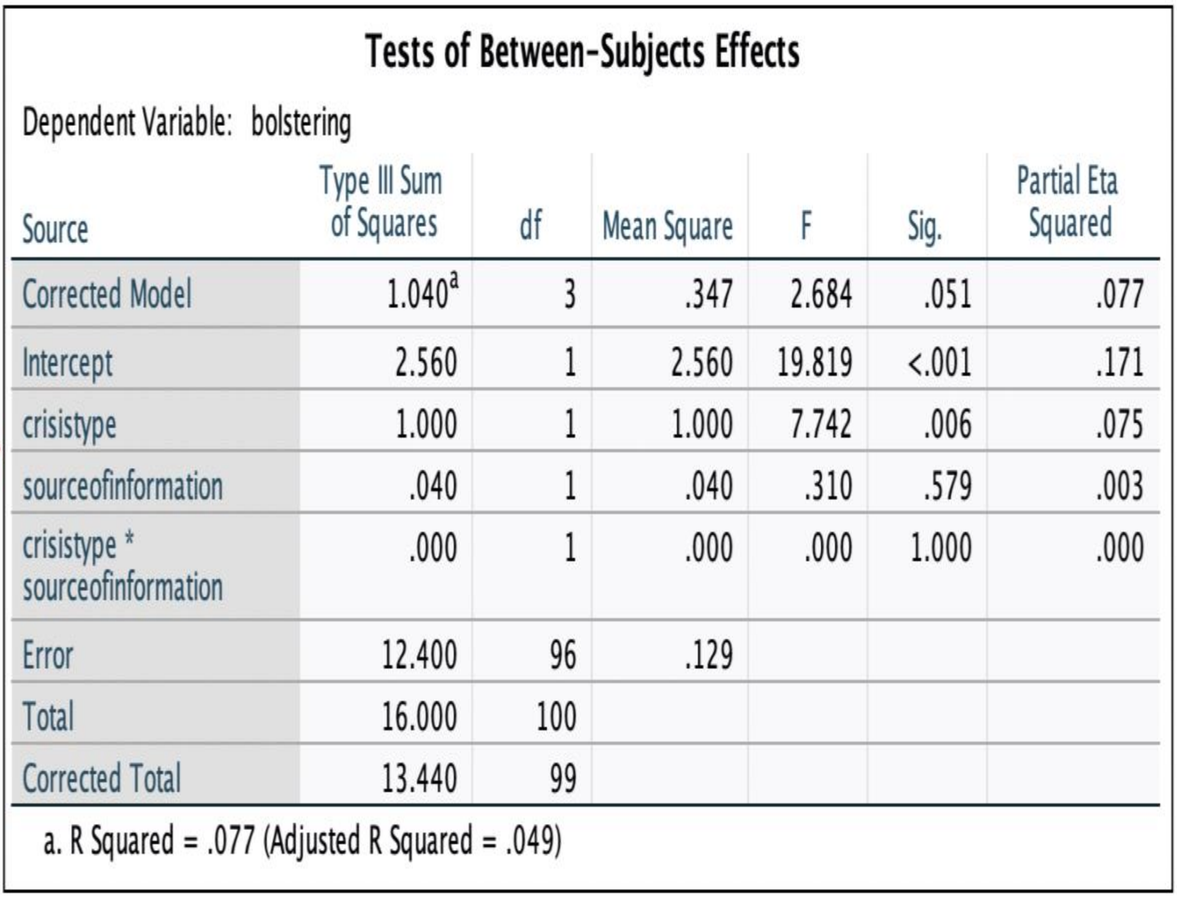
Dependent Variable: genuine remorse

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 4.400a | 3 | 1.467 | 7.184 | <.001 | .183 |
| Intercept | 36.000 | 1 | 36.000 | 176.327 | <.001 | .647 |
| crisistype | 1.000 | 1 | 1.000 | 4.898 | .029 | .049 |
| sourceofinformation | .160 | 1 | .160 | .784 | .378 | .008 |
| crisistype * sourceofinformation | 3.240 | 1 | 3.240 | 15.869 | <.001 | .142 |
| Error | 19.600 | 96 | .204 | | | |
| Total | 60.000 | 100 | | | | |
| Corrected Total | 24.000 | 99 | | | | |

a. R Squared = .183 (Adjusted R Squared = .158)

Table 12. tests of between – subject effects on dependent variable – genuine remorse

There was a significant difference between preventable and a victim organizational crisis on expressing a genuine remorse. The main effect of crisis type yielded an effect size of 0.049, indicating that 4,9% of variance in number of apologies was explained by crisis type (F (1, 96) =1.000, P=.029). However, there was no significant difference between the levels of source of information.



Tests of Between-Subjects Effects

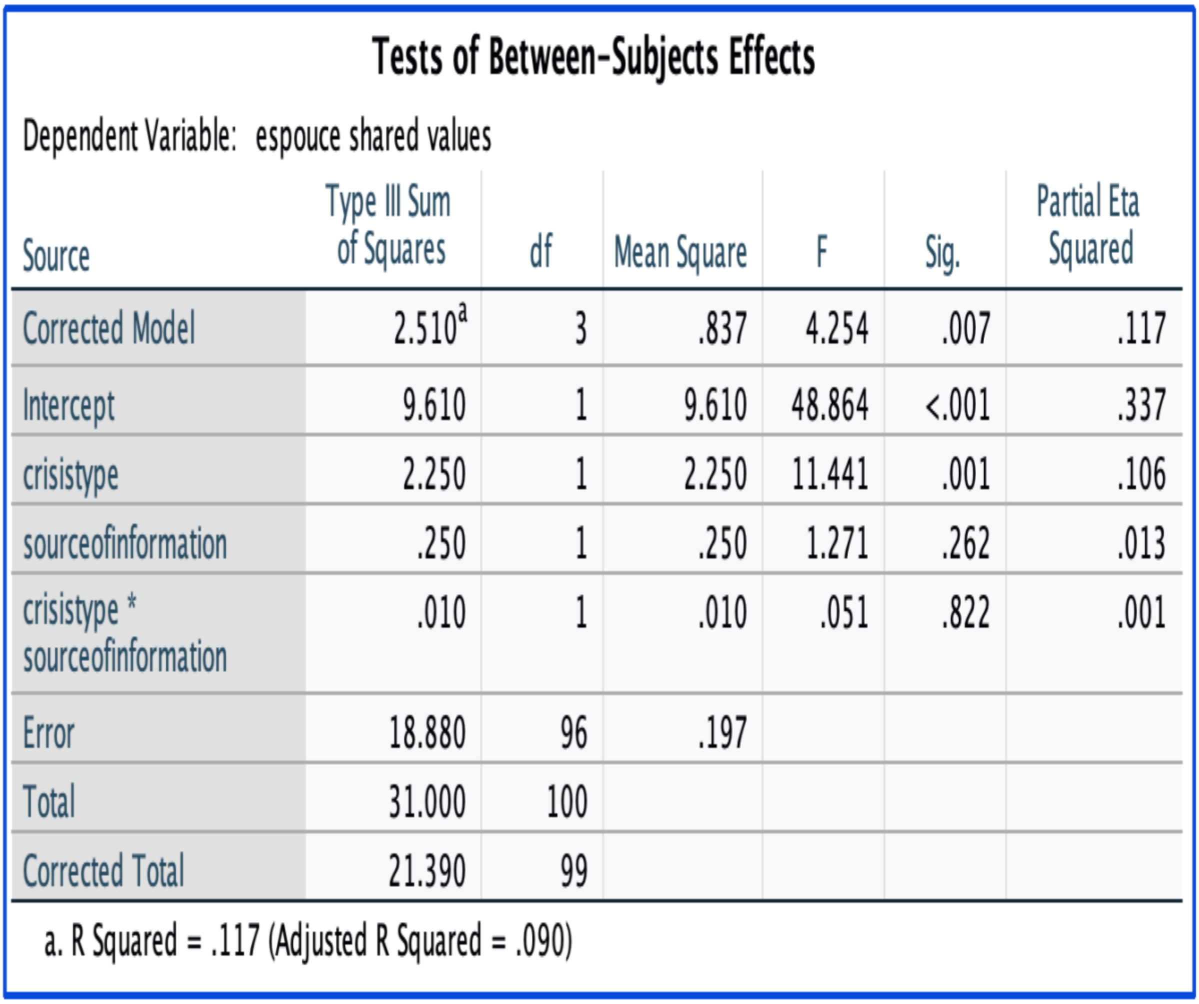
Dependent Variable: bolstering

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 1.040[a] | 3 | .347 | 2.684 | .051 | .077 |
| Intercept | 2.560 | 1 | 2.560 | 19.819 | <.001 | .171 |
| crisistype | 1.000 | 1 | 1.000 | 7.742 | .006 | .075 |
| sourceofinformation | .040 | 1 | .040 | .310 | .579 | .003 |
| crisistype * sourceofinformation | .000 | 1 | .000 | .000 | 1.000 | .000 |
| Error | 12.400 | 96 | .129 | | | |
| Total | 16.000 | 100 | | | | |
| Corrected Total | 13.440 | 99 | | | | |

a. R Squared = .077 (Adjusted R Squared = .049)

Table 13. tests of between – subject effects on dependent variable – bolstering

On the dependent variable – bolstering, there was a significant difference between preventable and victim organizational crisis. The main effect of crisis type yielded an effect size of 0.075, indicating that 7,5% of variance in number of apologies was explained by crisis type (F (1, 96) =1.000, P=.006). However, there was no significant difference between the levels of source of information.



Tests of Between-Subjects Effects

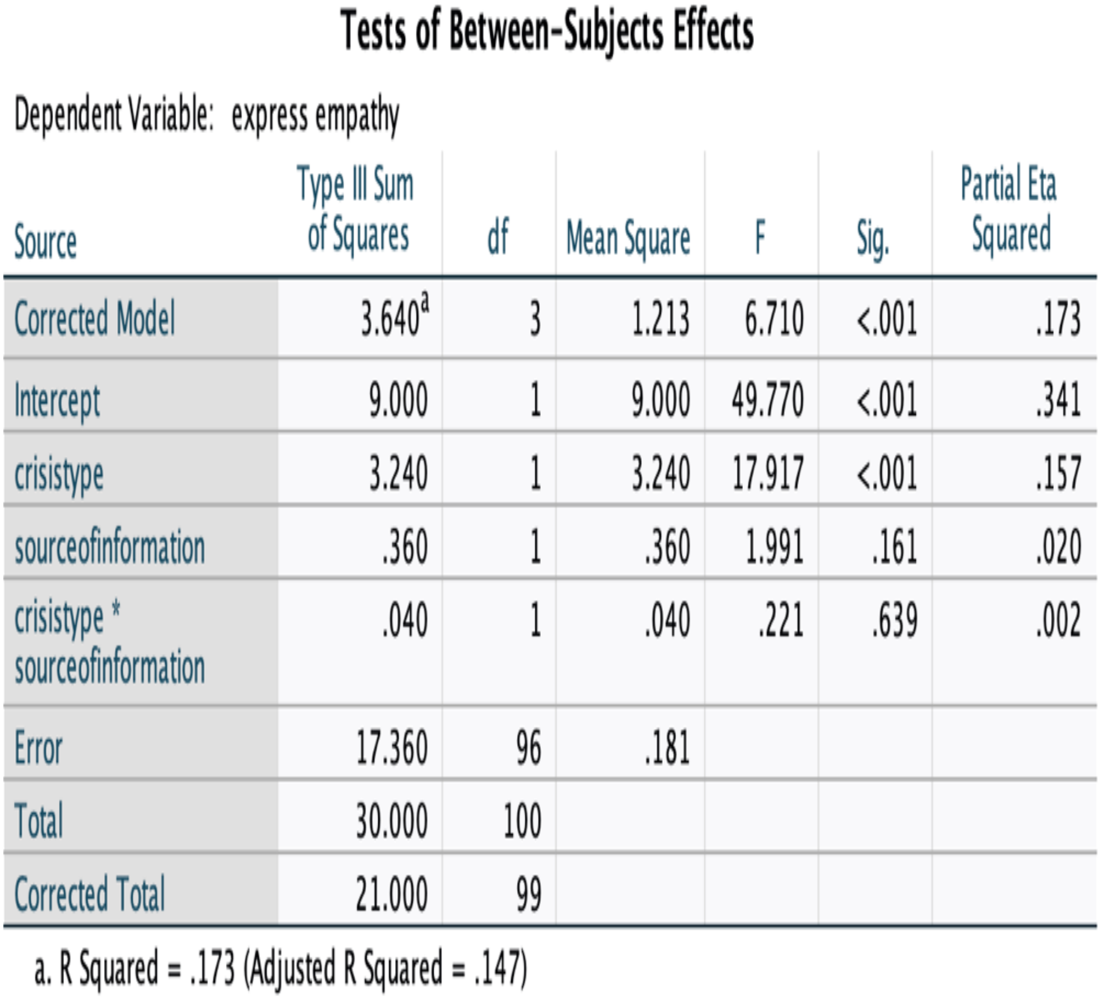
Dependent Variable: espouce shared values

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 2.510[a] | 3 | .837 | 4.254 | .007 | .117 |
| Intercept | 9.610 | 1 | 9.610 | 48.864 | <.001 | .337 |
| crisistype | 2.250 | 1 | 2.250 | 11.441 | .001 | .106 |
| sourceofinformation | .250 | 1 | .250 | 1.271 | .262 | .013 |
| crisistype * sourceofinformation | .010 | 1 | .010 | .051 | .822 | .001 |
| Error | 18.880 | 96 | .197 | | | |
| Total | 31.000 | 100 | | | | |
| Corrected Total | 21.390 | 99 | | | | |

a. R Squared = .117 (Adjusted R Squared = .090)

Table 14. tests of between – subject effects on dependent variable – espouse shared values

There was a significant difference between levels of type of crisis on espousal of shared values. The main effect of crisis type yielded an effect size of .106, indicating that 10,6% of variance in number of apologies was explained by type of crisis (F(1, 96) = 2.250, P=.001). However, there was no significant difference between levels of source of information.



Tests of Between-Subjects Effects

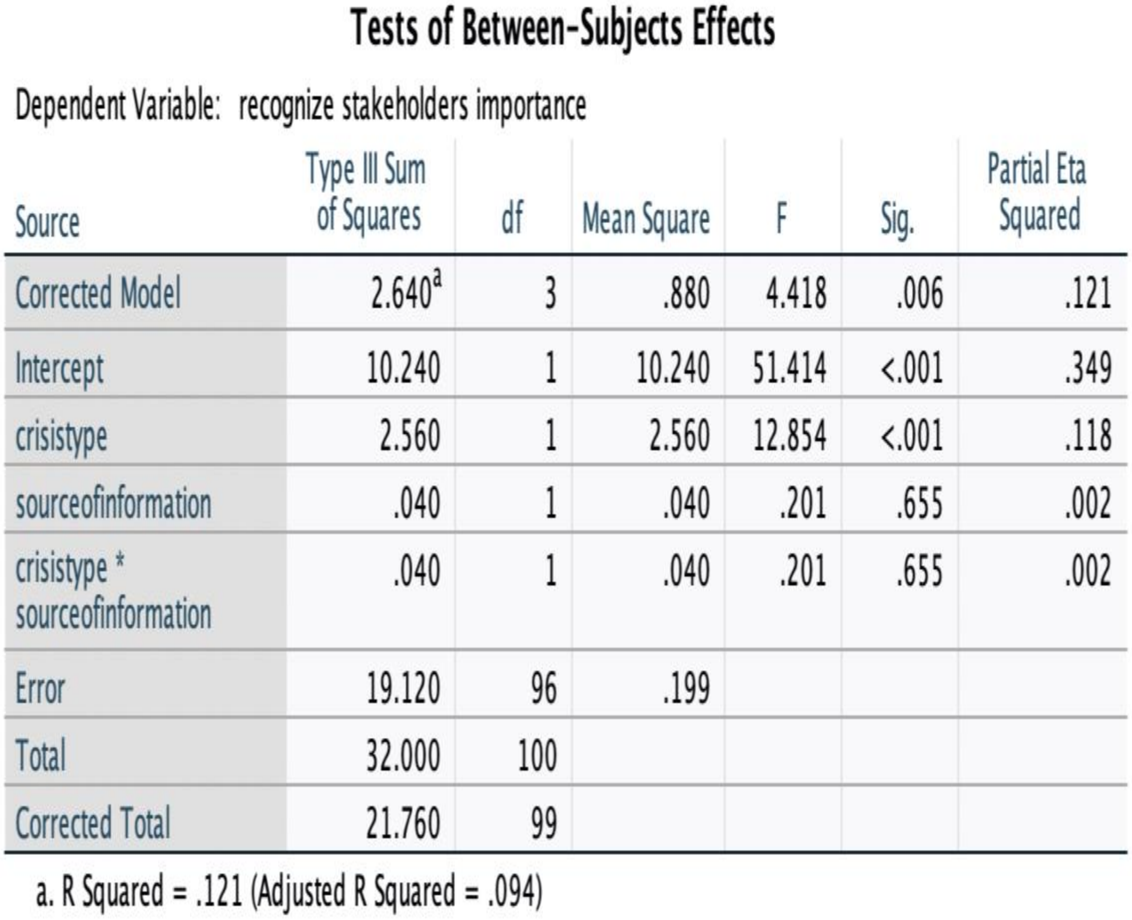
Dependent Variable: express empathy

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 3.640[a] | 3 | 1.213 | 6.710 | <.001 | .173 |
| Intercept | 9.000 | 1 | 9.000 | 49.770 | <.001 | .341 |
| crisistype | 3.240 | 1 | 3.240 | 17.917 | <.001 | .157 |
| sourceofinformation | .360 | 1 | .360 | 1.991 | .161 | .020 |
| crisistype * sourceofinformation | .040 | 1 | .040 | .221 | .639 | .002 |
| Error | 17.360 | 96 | .181 | | | |
| Total | 30.000 | 100 | | | | |
| Corrected Total | 21.000 | 99 | | | | |

a. R Squared = .173 (Adjusted R Squared = .147)

Table 15. tests of between – subject effects on dependent variable – express empathy

There was a significant difference between the levels of type of crisis on expressing empathy. The main effect of crisis type yielded an effect size of .157, indicating that 15,7% of variance in number of apologies was explained by the crisis type (F (1, 96) =3.240, P<.001). There was no significant difference between the levels of source of information.



Tests of Between-Subjects Effects

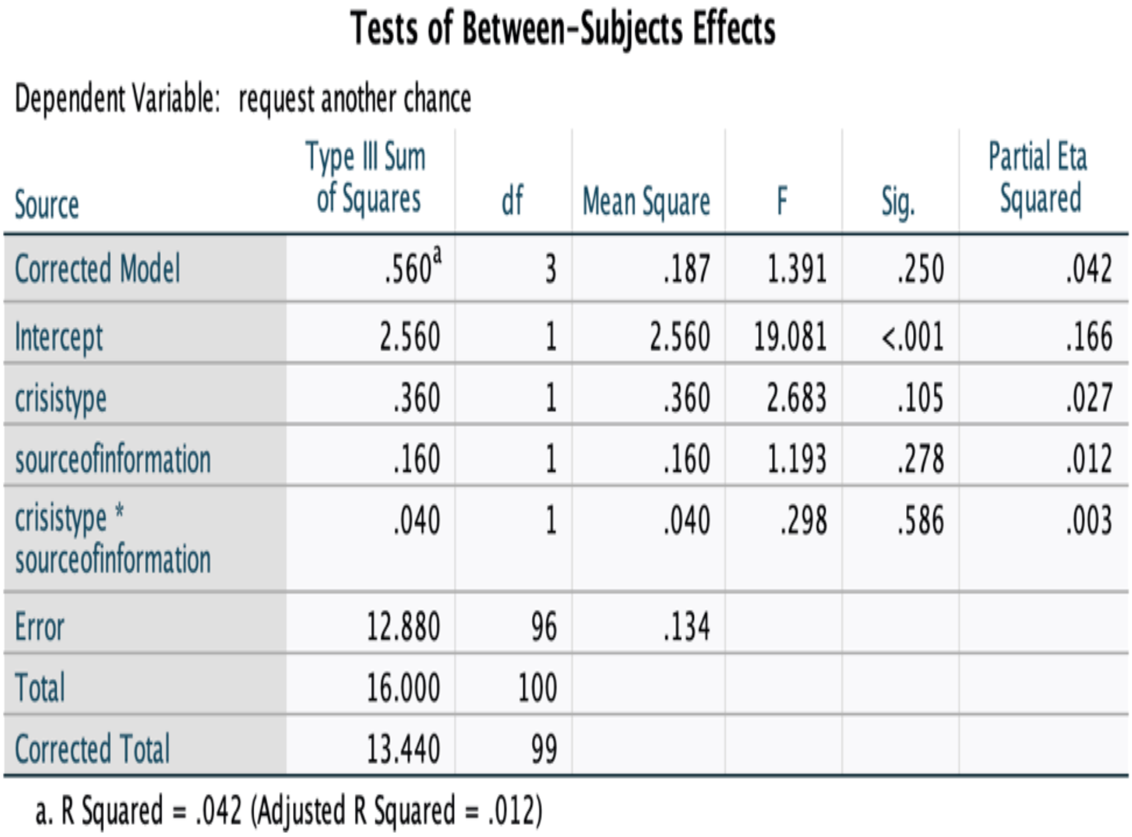
Dependent Variable: recognize stakeholders importance

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 2.640[a] | 3 | .880 | 4.418 | .006 | .121 |
| Intercept | 10.240 | 1 | 10.240 | 51.414 | <.001 | .349 |
| crisistype | 2.560 | 1 | 2.560 | 12.854 | <.001 | .118 |
| sourceofinformation | .040 | 1 | .040 | .201 | .655 | .002 |
| crisistype * sourceofinformation | .040 | 1 | .040 | .201 | .655 | .002 |
| Error | 19.120 | 96 | .199 | | | |
| Total | 32.000 | 100 | | | | |
| Corrected Total | 21.760 | 99 | | | | |

a. R Squared = .121 (Adjusted R Squared = .094)

Table 16. tests of between – subject effects on dependent variable - recognize stakeholders’ importance

There was a significant difference between the levels of type of crisis on recognition of stakeholders` importance. The main effect of  a crisis type yielded an effect size of .118, indicating that 11,8% of variance in number of apologies was explained by a crisis type (F (1, 96) =2.560, P<.001). There was no significant difference between the levels of source of information.



**Tests of Between-Subjects Effects**

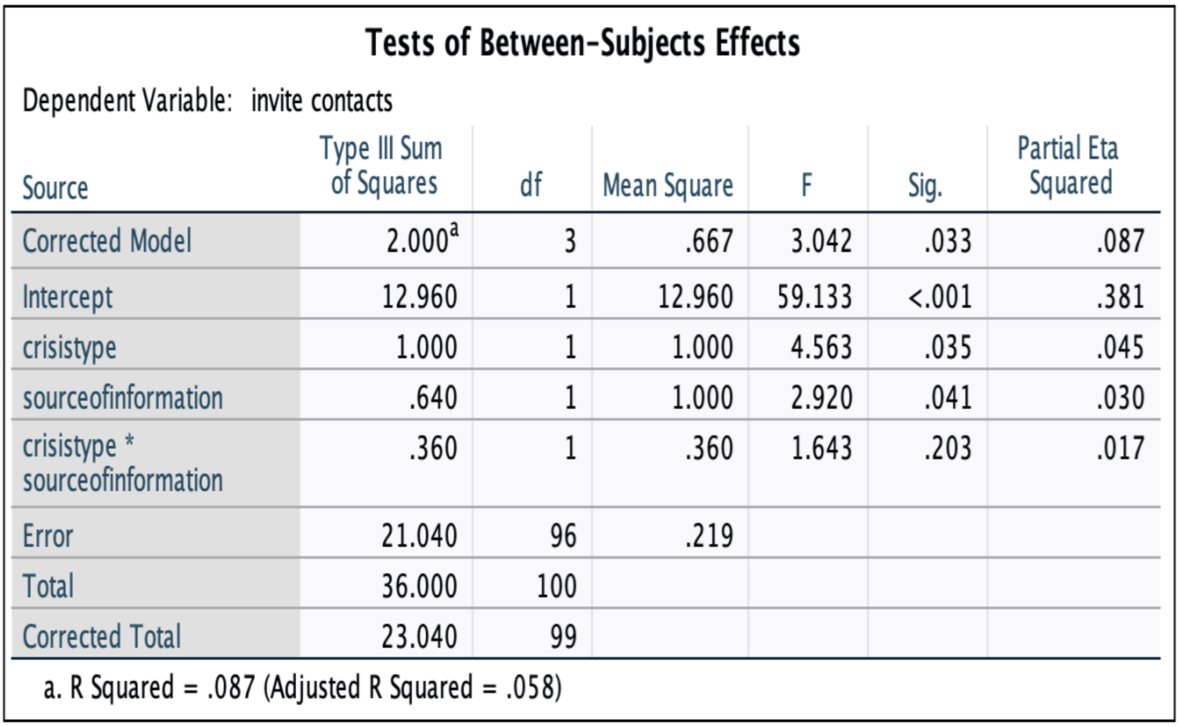
Dependent Variable: request another chance

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | .560[a] | 3 | .187 | 1.391 | .250 | .042 |
| Intercept | 2.560 | 1 | 2.560 | 19.081 | <.001 | .166 |
| crisistype | .360 | 1 | .360 | 2.683 | .105 | .027 |
| sourceofinformation | .160 | 1 | .160 | 1.193 | .278 | .012 |
| crisistype * sourceofinformation | .040 | 1 | .040 | .298 | .586 | .003 |
| Error | 12.880 | 96 | .134 | | | |
| Total | 16.000 | 100 | | | | |
| Corrected Total | 13.440 | 99 | | | | |

a. R Squared = .042 (Adjusted R Squared = .012)

Table 17. tests of between – subject effects on dependent variable – request another chance

There was no significant difference in neither the levels of type of crisis nor the levels of source of information on the dependent variable - requesting another chance.



**Tests of Between-Subjects Effects**

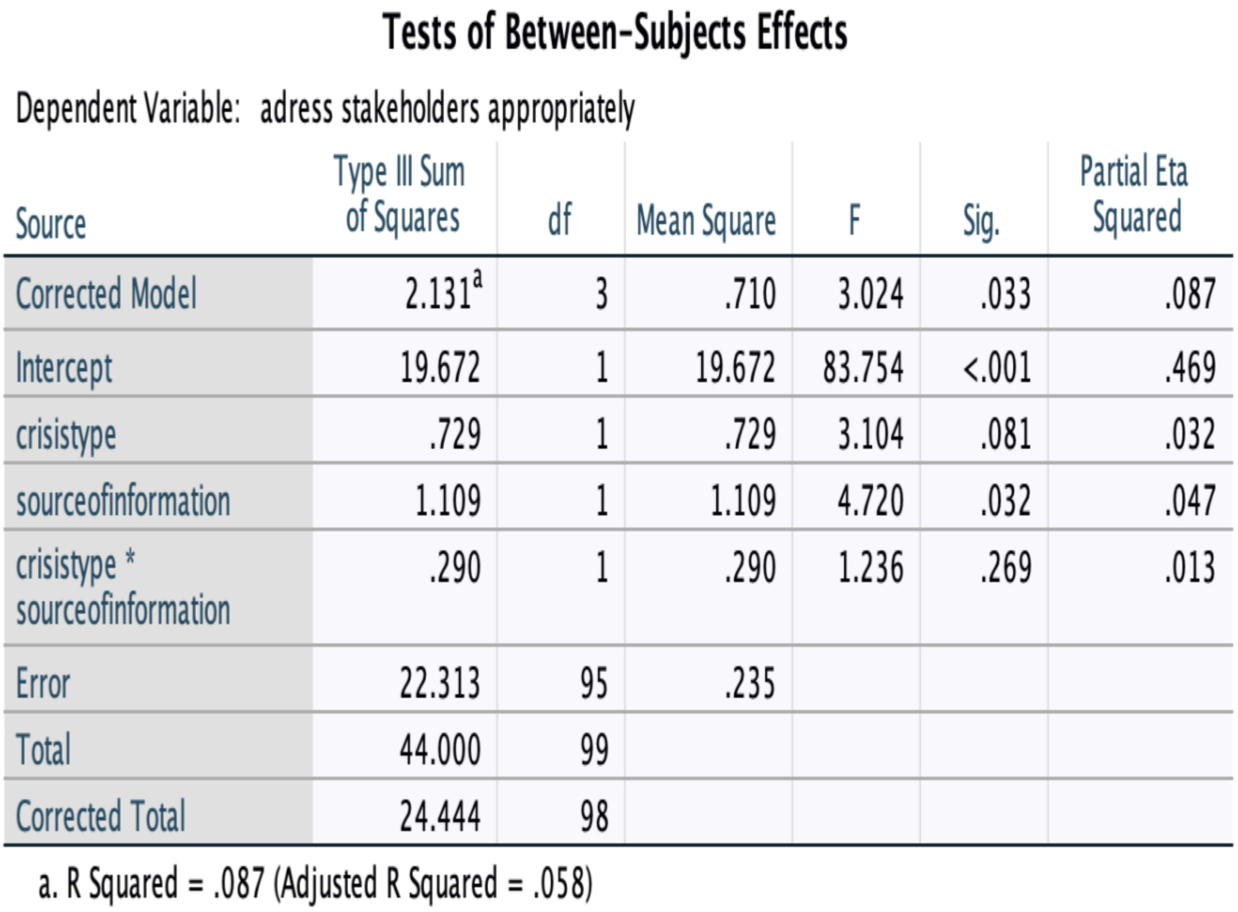
Dependent Variable: invite contacts

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 2.000[a] | 3 | .667 | 3.042 | .033 | .087 |
| Intercept | 12.960 | 1 | 12.960 | 59.133 | <.001 | .381 |
| crisistype | 1.000 | 1 | 1.000 | 4.563 | .035 | .045 |
| sourceofinformation | .640 | 1 | 1.000 | 2.920 | .041 | .030 |
| crisistype * sourceofinformation | .360 | 1 | .360 | 1.643 | .203 | .017 |
| Error | 21.040 | 96 | .219 | | | |
| Total | 36.000 | 100 | | | | |
| Corrected Total | 23.040 | 99 | | | | |

a. R Squared = .087 (Adjusted R Squared = .058)

Table 18. tests of between – subject effects on dependent variable – invite contacts

There was significant difference between  the levels of type of crisis and source of information. The main effect of crisis type yielded an effect size of 0.045, indicating that 4,5% of variance in number of apologies was explained by crisis type (F (1, 96) =1.000, P=.035). The main effect of the source of information yielded an effect size of 0.030, indicating that 3% of variance in number of apologies was explained by crisis type (F (1, 96) =1.000, P=.041).



Tests of Between-Subjects Effects

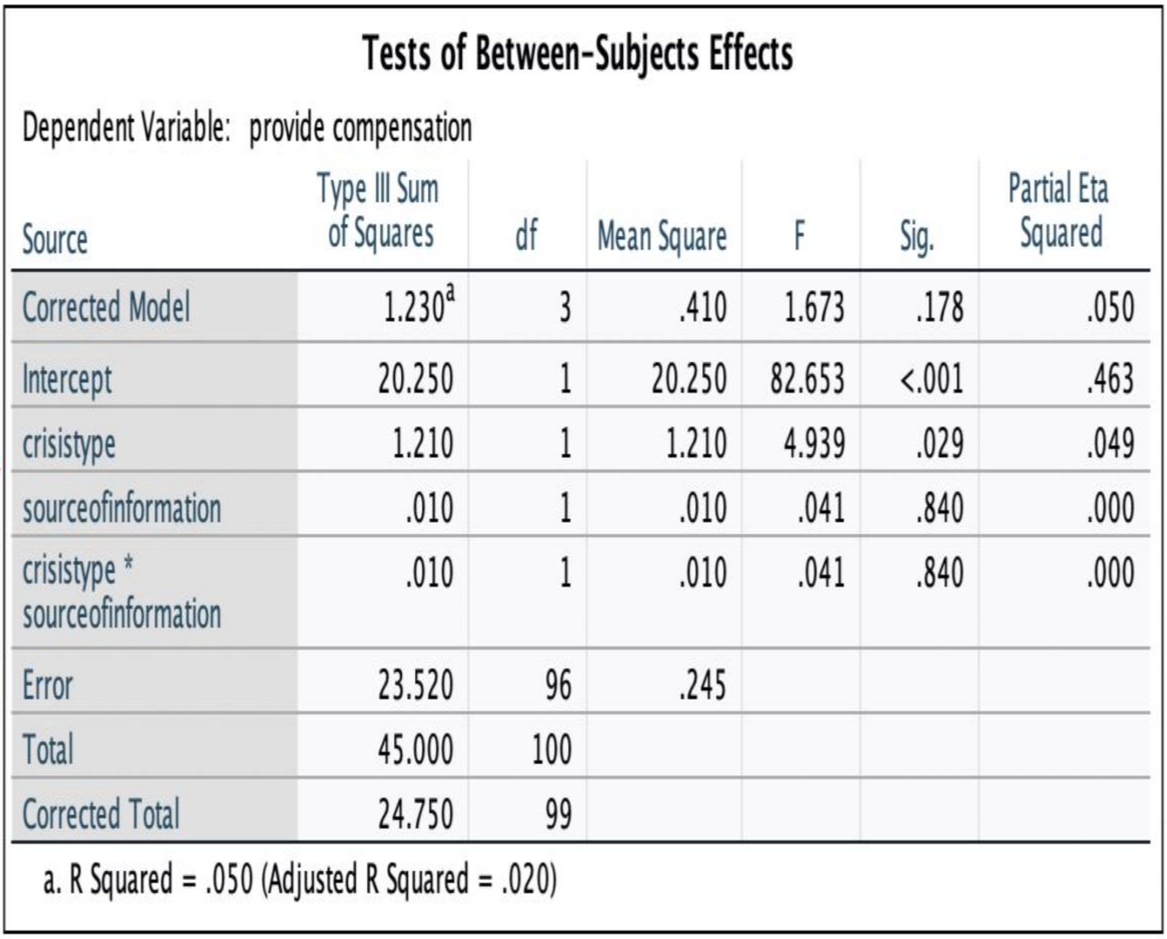
Dependent Variable:   adress stakeholders appropriately

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 2.131[a] | 3 | .710 | 3.024 | .033 | .087 |
| Intercept | 19.672 | 1 | 19.672 | 83.754 | <.001 | .469 |
| crisistype | .729 | 1 | .729 | 3.104 | .081 | .032 |
| sourceofinformation | 1.109 | 1 | 1.109 | 4.720 | .032 | .047 |
| crisistype * sourceofinformation | .290 | 1 | .290 | 1.236 | .269 | .013 |
| Error | 22.313 | 95 | .235 | | | |
| Total | 44.000 | 99 | | | | |
| Corrected Total | 24.444 | 98 | | | | |

a. R Squared = .087 (Adjusted R Squared = .058)

Table 19. tests of between – subject effects on dependent variable – address stakeholders appropriately

There was no significant difference between levels of type of crisis on the effect of dependent variable - addressing stakeholders appropriately. However, there was a significant difference between levels of source of information. The main effect of source of information yielded an effect size of 0.047, indicating that 4,9% of variance in number of apologies was explained by crisis type (F (1, 96) =1.109, P=.032).



Tests of Between-Subjects Effects

Dependent Variable: provide compensation

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. | Partial Eta Squared |
|---|---|---|---|---|---|---|
| Corrected Model | 1.230[a] | 3 | .410 | 1.673 | .178 | .050 |
| Intercept | 20.250 | 1 | 20.250 | 82.653 | <.001 | .463 |
| crisistype | 1.210 | 1 | 1.210 | 4.939 | .029 | .049 |
| sourceofinformation | .010 | 1 | .010 | .041 | .840 | .000 |
| crisistype * sourceofinformation | .010 | 1 | .010 | .041 | .840 | .000 |
| Error | 23.520 | 96 | .245 | | | |
| Total | 45.000 | 100 | | | | |
| Corrected Total | 24.750 | 99 | | | | |

a. R Squared = .050 (Adjusted R Squared = .020)

Table 20. tests of between – subject effects on dependent variable – provide compensation

There was a significant difference between the levels of crisis type on providing compensation. The main effect of crisis type yielded an effect size of 0.049, indicating that 4,9% of variance in number of apologies was explained by crisis type (F (1, 96) =1.210, P=.029). There was no significant difference between the levels of source of information on providing compensation.

# 5 Discussion and Conclusion

## 5.1 Research Question 1

As already discussed, what constitutes an apology varies between scholars, but it is generally agreed that there are essential components to a complete corporate apology.

The first research question asked what elements of an organizational apologies are important in reestablishing social legitimacy with stakeholders in victim and preventable types of crises. Participants in this research associated apologies with the acknowledgment of responsibility, mitigating harm, offering reparations, expressing genuine remorse, bolstering, espousing shared values, expressing empathy, emphasizing stakeholders' importance, requesting another chance, inviting contacts, addressing stakeholders appropriately and providing compensations, offering explanation and telling stakeholders what actions to take and how to prevent reoccurrence.

As reported by Kellerman (2006), apology is the most complex and controversial of the crisis response strategies. It is crucial to differentiate between full and partial apologies. A full apology must acknowledge the crisis, accept responsibility, include a promise not to repeat crisis, and concern and regret. A partial apology is typically just an expression of concern and regret (p.156).

This study suggests that in the case of data breach partial apologies will not satisfy stakeholders needs after crisis. Almost all apologies written by participants contained either the word "apologize" or the word "sorry." More interesting is that majority of participants used adverbs such as "sincerely," "deeply," or "truly," or "really," "extremely," "incredibly," "from the bottom of our heart" to intensify the apology. However, what is revealed is that stakeholders want organizations to take further measures which should be reflected in the words and behaviors. It must be noted that the most frequently mentioned elements of apologies by participants were the following: expressing genuine remorse, preventing reoccurrence, corrective action and providing compensation.

According to Coombs/Schmidt (2000), when the representatives of the organization apologize, they accept responsibility for the crisis. Compensation promotes the acceptance of responsibility by offering monetary reparations. Furthermore, corrective action involves identifying and fixing the source of the crisis. Corrective action can also be seen as an acceptance of responsibility for a crisis, because when an organization identifies and then eliminates the cause of the crisis, this process can be seen as efforts from the side of the organization to prevent reoccurrence of the crisis.

As a whole, stakeholders want a combination of words and behaviors that focus on fixing the problem as well as rebuilding the relationship. However, apologies in the four scenarios differ in quantity regarding the type of crisis (victim or preventable) as well as source of information (organization or media).

Only one participant in the second scenario wrote that they have never conducted online transactions: "I have never conducted online business and I never will. That is all I have to add here and I cannot help you with your task. It is exactly because I know about internet security, that I do not purchase things online.''

### 5.2 Research Question 2

The second question asked whether there was a significant difference between victim an preventable types of crisis considering the apologies constructed by stakeholders.

As already mentioned, apologies written by participants differed in quantity and content regarding the type of crisis and a source of information about the breach. It is worth noting that after conducting factorial ANOVA (two – way ANOVA) there was a significant difference between preventable and victim organizational crisis considering the number of apologies mentioned by the stakeholders, (F (1, 96) =33.201, P<001).

Furthermore, related to each mentioned apology, there was also a significant difference between preventable and victim organizational crisis on acknowledging responsibility, mitigating harm, offering reparations, expressing genuine remorse, bolstering, espousing shared values, expressing empathy, emphasizing stakeholders' importance, requesting another chance, inviting contacts, addressing stakeholders appropriately and providing compensations. Exemptions were offering explanation, telling stakeholders what actions to take and and how to prevent reoccurrence. There was no significant difference between victim and preventable organizational crisis on the effect of the three above-mentioned apologies.

Furthermore, in those cases where the breach was caused by an employee (preventable types of crises) numbers of apologies written by stakeholders (categorized in problem fixing themes and relationship rebuilding themes) were higher than in those cases where breach was caused by a hacker (victim type of crisis).

In general, in the second and third scenarios where the breach was caused by the employee, more participants required the organization to acknowledge responsibility, to mitigate harm, offer reparation as well as prevent reoccurrence of the crisis. Besides, more participants in the same scenarios wanted to see genuine remorse and empathy from the organization, as well as the company to recognize the customer´s importance and espouse shared values. Furthermore, in preventable organizational crisis more stakeholders wanted organization to ask for another chance, provide compensation and to hear about organization´s past good deeds. These apologies were also seen in those scenarios where the breach was caused by a hacker, however less so than in other scenarios.

There were some apologies where the differences in frequencies of apologies written by stakeholders are more obvious. For example, in the Table 3. and Table 4. in the problem fixing themes, stakeholders seemed to be more demanding when it comes to acknowledging the responsibility than in those scenarios where an employee is responsible for the breach in the organization. In the second (40%) and third (32%) scenarios where the breach was caused by the employee, there are twice as many apologies showing the desire for the organizations to express the sense of responsibility about the occurred crisis as in the first (12%) and fourth (20%) cases, where the breach was caused by a hacker.

When it comes to corrective action, stakeholders participating in those scenarios where the breach was caused by an employee of an organization turned out to be more demanding than in those scenarios where the crisis occurred by an intervention of a hacker. This element was evident in fifty two (52% ) and forty eight (48%) percent of written statements in preventable types of crisis and only in sixteen (16%) and twenty four (24%) percent of responses in those scenarios where the breach was caused by a hacker. For instance, in those scenarios where an employee committed a crime, some statements included the following content: “We want to make clear that it was only one of our employees who is no longer working here and will have to face legal consequences.”

Regarding the relationship rebuilding themes, there are also some obvious differences in specific themes. For instance, in those scenarios where the breach was caused by an employee, more stakeholders were willing for the organizations to express concern and empathy (56%, 44%) and to recognize their importance as customers (52%,44%). Comparatively, in the two other scenarios where the breach was caused by a hacker, the express of concern and empathy (8%,16%) and recognition of their importance as customers (12%,12%) was shown in less quantity. Regarding providing compensation, there was still a slight difference between the numbers of apologies used by stakeholders.

### 5.3 Research Question 3

Research question 3 asked whether there was significant difference between the levels of source of information (organization vs. media) considering the apologies constructed by stakeholders.

When an organization is the source of information about an occurred crisis, there is a less reputational damage than if the news media are the first to deliver the information. This effect has been called “stealing thunder” ( Arpan & Pompper, 2004, p.295).

It is worth mentioning, that after conducting factorial ANOVA (two – way ANOVA) there was significant difference between the levels of source of information (organization or media) on the number of apologies mentioned by the stakeholders, (F (1, 96) = 8.652, P =.004).

When considering each mentioned apology separately, there was also a significant difference between the levels of source of information in the terms of mitigating harm, inviting contacts, and addressing stakeholders appropriately.

In preventable as well as in victim organizational crisis where the source of information about the crisis was media, the stakeholders were obviously having more desire for the organization to offer them explanations about the occurred crisis and to foster personal communication. The desire of explanation was seen in thirty two percent (32%) of written apologies in the second scenario and thirty six percent (36%) of apologies in the fourth scenario. Concerning fostering personal communication, stakeholders desire organizations to contact was apparent in the second scenario with forty six percent (46%) of apologies and in forty four percent (44%) in the fourth scenario. While in those scenarios where the stakeholders found out about the crisis directly from the organization, only twelve percent (12%) of the participants in the first scenario and twenty four percent (24%) in the third scenario wanted to hear further explanations about the occurred crisis. Only twelve percent (20%) of the participants in the first scenario and thirty six percent (36%) in the third scenario, wanted organization to foster personal communication with them. It is worth noting further that in this case a type of crisis did not play a vital role. It turned out that the fact of whether the breach was caused by a hacker or an employee itself did not matter when it came to providing explanation about the occurred crisis and fostering personal communication. Whether the stakeholder learned about the crisis from the organization or the media played more important role. One participant in the scenario, who found out about the breach from the internet, wrote: “We are sincerely sorry for what has happened. On behalf of my team, I wanted to reach out to you personally (!) and offer you - if you so wish - insight in some of the things that have happened.”

### 5.4 General Discussion

An organization faces various challenges during a crisis. One of the challenges is to protect and rebuild an organization's reputation and reestablish its social legitimacy. According to Coombs (2012) " crisis type generates specific and predictable levels of crisis responsibility-attributions of organizational responsibility for the crisis "( p.168). The aim of this study is to analyze definitions of apologies and explore the elements of an effective organizational apology in preventable and victim organizational crisis from the stakeholders' perspective. Furthermore, the study explored whether there was a significant difference between preventable and victim organizational crisis and between different sources of information (media vs. organization) considering apologies written by stakeholders. After conducting a factorial ANOVA (two – way ANOVA), the results showed that there was a significant difference between the preventable and victim organizational crisis, as well as the significant difference between difference levels of source of information (media vs. organization) on apologies constructed by stakeholders. It is worth mentioning that in the crisis with different attribution levels, stakeholders expected organizations to provide them with apologies which differed in context and most importantly – in quantity. More specifically, as expected, the stakeholders had more expectations from those organizations where the breach was caused by an employee. Most of apologies in the problem fixing themes and relationship rebuilding themes given in the Tables 3, 4 and 5 were presented in higher numbers in the responses of those scenarios where the crisis was caused by an employee. Besides, the source of information – the way stakeholders were informed about the crisis, also played a vital role, which proves that how and when organizations communicate about the crisis with its stakeholders also plays an important role in saving organization´s reputation.

### 5.5 Theoretical Implications

Three factors are used in SCCT to evaluate the reputational threat presented by a crisis: crisis type, crisis history, and prior reputation. The first step is to determine the crisis type - the frame that is used to interpret the crisis. Research proves that each crisis type has its own attribution level in the eyes of stakeholders. The victim cluster produces very little crisis responsibility for an organization. Stakeholders see the organization as a victim of the crisis, not the cause of the crisis. The accident cluster produces low attributions of organizational crisis responsibility. The preventable cluster produces very strong attributions of organizational crisis responsibility (Coombs, 2012, p.157). The result of this study suggests that there is a significant difference between preventable and victim organizational crisis considering the apologies constructed by stakeholders.

For example, in those scenarios where the breach was caused by an employee, more participants required from the organization to acknowledge the responsibility, mitigate harm, offer reparation as well as prevent reoccurrence of the crisis. Besides, more participants in the same scenarios wanted to hear genuine remorse and empathy from the organization, as well as for the organization to recognize their importance and espouse shared values. Furthermore, in preventable organizational crisis more stakeholders wanted organization to request another chance, provide compensation and to hear about organizations' past good deeds.

Crisis responsibility can be a threat to an organizations' reputation because stronger attributions of crisis responsibility produce greater reputational damage. If the crisis type is ambiguous, the crisis team can attempt to shape which frame is selected. However, there is possibility that the crisis team and stakeholders might have a disagreement on the crisis type. If this is the case the crisis team should seriously consider the stakeholders' frame (Coombs, 2012, p.157). This study explored stakeholders' perception of apologies in organizational crisis where the case was a data breach, which is somewhat of an ambiguous crisis. Accordingly, it was interesting to examine what attribution level do stakeholders regard a crisis (data breach) to carry when it is caused by different reasons - in this case - when breach was caused by an employee or by a hacker. As expected, stakeholders attributed much more responsibility to those organizations where the breach was caused by an employee of this company.

In the framework of crisis communication, stealing thunder is an admission of a weakness (usually a mistake or failure) before that weakness is announced by another party, such as an interest group or the media. In organizational settings, stealing thunder' s efficiency has been demonstrated among potential consumers. For example, consumers' negative attitude of an organization can be lessened by disclosing information about failure and mistakes done. For an organization to steal thunder in a crisis situation, it must break the news about its own crisis, rather than waiting to respond to inquiries from the media or other key publics. (Arpan, Pompper, 2003, p.294).

This study stated that there was a significant difference between the levels of source of information considering apologies written by stakeholders. This study also suggested that when stakeholders were informed about the crisis from the media, more of them preferred apologies to come specifically from organization, to be addressed by name and and to be invited  to contact the organization in case they had any further question about the occurred crisis.

### 5.6 Practical implications

This study suggests that stakeholders look for a combination of words and behaviors in organizational apologies. It also suggests that apologies should concentrate on both fixing problems and rebuilding relationships. Besides, this study identifies a number of different elements that can be included in an effective apology in order organization to rebuild its reputation relationships with stakeholders and reassert social legitimacy. However, a crisis type and a quick response play an important role when organizations try to manage the crisis. The present findings suggest that stakeholders' expectations differ between victim and preventable organizational crisis and that there is less reputational damage when an organization is the information source about a crisis occurring than if the news media are the first to deliver the information.

### 5.7 Limitations and Suggestions for Future Study

This study has several limitations. First, it used a hypothetical scenario of data breach, that is why it is possible that participants were not as emotionally involved as they would have been in real life. Real feelings of anger or fear might change the way stakeholders view an apology. Second, categories presented in this study were tested experimentally. Accordingly, the researcher may not have understood all the data provided the way the participants intended. Furthermore, there is a possibility that the themes and categories identified may not be generalized to other populations as stakeholders might expect an apology to be constructed differently in other situations.

Future research might give stakeholders the opportunity to construct organizational apologies in different scenarios of organizational crisis with different attribution level of responsibility to see whether there is significant difference between various types of crisis.

Identifying the crisis type enables an initial assessment of the amount of crisis responsibility that public will attribute to a crisis situation. Adjustments are then made to this initial assessment by considering two factors, severity and performance history. Severity is the amount of damage generated by a crisis including financial, human, and environmental damage. Performance history indicates to the past actions or conduct of an organization including its crisis history (whether an organization has had previous crises) and relationship history (especially how well or poorly it has treated stakeholders). (Coombs & Holladay, 2002, p.169). Future research might also give participants opportunity to write apologies for the crisis where the real organization will be included, and a performance history of this organization will also be considered.

## 5.8 Conclusion

Crises are costly, but they can be more costly in case of managing them improperly. When organizational faces crisis, managers must be ready to respond appropriately. Managers cannot unilaterally decide what an appropriate response is. On the contrary, they must consider their stakeholders' needs and expectations. Besides, crisis differ in its severity and attribution level of responsibility, which means that managers should realize that stakeholders might have more expectations from the organization that carries strong attribution level of crisis responsibility. Furthermore, the way organization communicates with stakeholders during a crisis plays an important role in the process of handling crisis, restoring the reputation of organization and reestablishing its´ social legitimacy.

## 6 References

Ayygari, R. (2012). An exploratory analysis of data breaches from 2005 – 2011: trends and insights. *Journal of Information Privacy & Security.*

Arpan, M.L., Pompper, D. (2003). Stormy weather: testing "stealing thunder" as a crisis communication strategy to improve communication flow between organizations and journalists, *Public Relations Review*, 29, 291–308.

Benoit, W. L. (2014). Accounts, Excuses, and Apologies, Second Edition : Image Repair Theory and Research (2nd ed.).: Image Repair Theory and Research

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

Bentley. M. J. (2018). What Counts as an Apology? Exploring Stakeholder Perceptions in a Hypothetical Organizational Crisis. *Communication Quarterly, 32, 202- 232*

Buckley, J., & Eberts, F. S., (1996*).* All I need to know about crisis control I learned in kindergarten*. Corporate Legal Times.*

Bradford, J. L., & Garrett, D. E. (1995). The effectiveness of corporate communicative responses to accusations of unethical behavior. *Journal of Business Ethics, 14*, 875-892.

Brock, T. C., & Brannon, L. A. (1992). Liberalization of commodity theory. *Basic and Applied Social Psychology, 13*(1), 135–144

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.

Clarkson, B. E. M. (1995). A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance. *The Academy of Management Review*, 92–117.

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

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, 165-186 .

Coombs, W. T., & Holladay, S. J.(2010). *The Handbook of Crisis Communication*, Oxford, England: Wiley-Blackwell.

Coombs, W. T. (2012). *Ongoing crisis communication: Planning, managing, and responding.* (3rd ed.). Los Angeles, CA: Sage.

Coombs, W. T. (2015). *Ongoing crisis communication: Planning, managing, and responding* (4th ed.). Thousand Oaks, CA: SAGE.

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

Dowling, J., & Pfeffer, J. (1975). Organizational legitimacy: Social values and organizational behavior. *The Pacific Sociological Review*, *18*, 122-136.

Ferrell, O. C. (2004). Business ethics and customer stakeholders. The Academy of Management Executive (1993-2005), 18, 126-129.

Griffin, M., Babin, B. J., & Attaway, J. S. (1991). An empirical investigation of the impact of negative public publicity on consumer attitudes and intentions. In R. H. Holman & M. R.

Soloman (Eds.), *Advances in consumer research* (Vol. 18, pp. 334-341). Provo, UT: Association for Consumer Research.

Hearit, K. M (1995). "Mistakes were made": Organizations, apologia, and crisis of social legitimacy. Communicaiton studies, Proquest 1 -17.

Hearit, K. M. (2006). *Crisis management by apology: Corporate response to allegations of wrongdoing*. Mahwah, NJ: Lawrence Erlbaum.

Kellerman B.(2006). When should a leader apologize and when not? Harv Bus Rev.

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

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

Metzler, M. S. (2001). The centrality of organizational legitimacy to public relations practice. In R. L. Heath (Ed.), *Handbook of public relations* (pp. 321-333). Thousand Oaks, CA: SAGE.

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*, 219-227.

Patel, A., & Reinsch, L. (2003). Companies can apologize: Corporate apologies and legal liability. *Business Communication Quarterly, 66*, 17-26.

Shuman, D. (2000). *Judicature*, 83, 186.

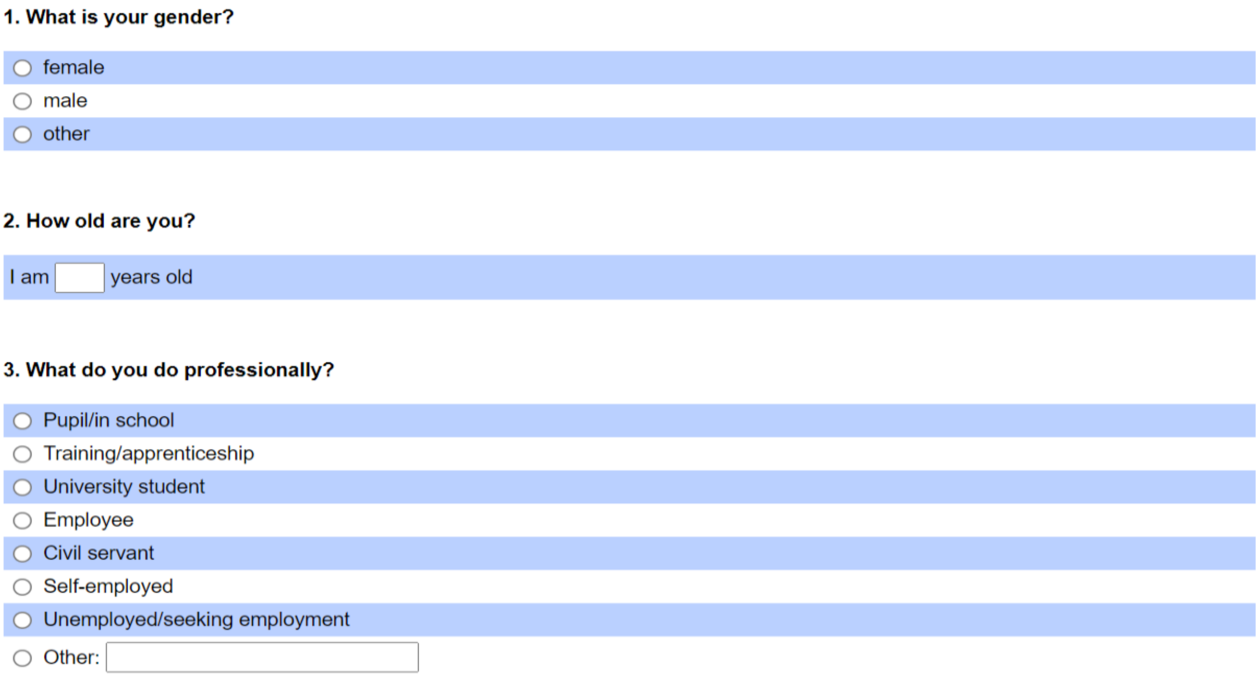
Thomas, R. L., & Millar, M. (2008). The impact of failing to give an apology and the need-for-cognition on anger. *Current Psychology, 27*, 126-134.

Weiner, B. (1986). *An attributional theory of motivation and emotion*. New York: Springer.

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

# 7 Appendix

Survey Questionnaire



**1. What is your gender?**

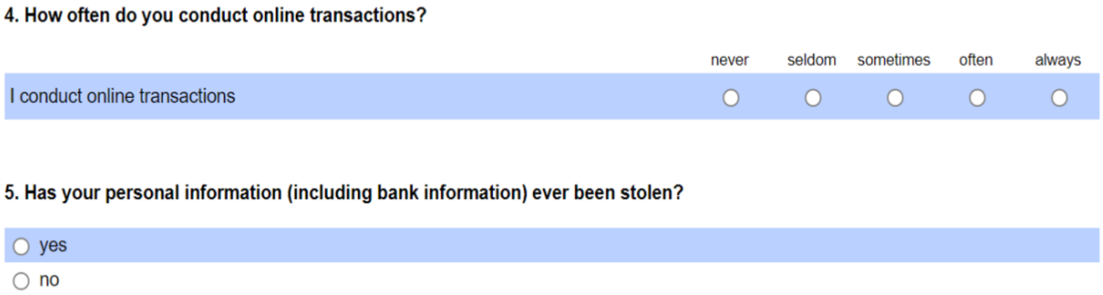
○ female
○ male
○ other

**2. How old are you?**

I am ▭ years old

**3. What do you do professionally?**

○ Pupil/in school
○ Training/apprenticeship
○ University student
○ Employee
○ Civil servant
○ Self-employed
○ Unemployed/seeking employment
○ Other: ▭



**4. How often do you conduct online transactions?**

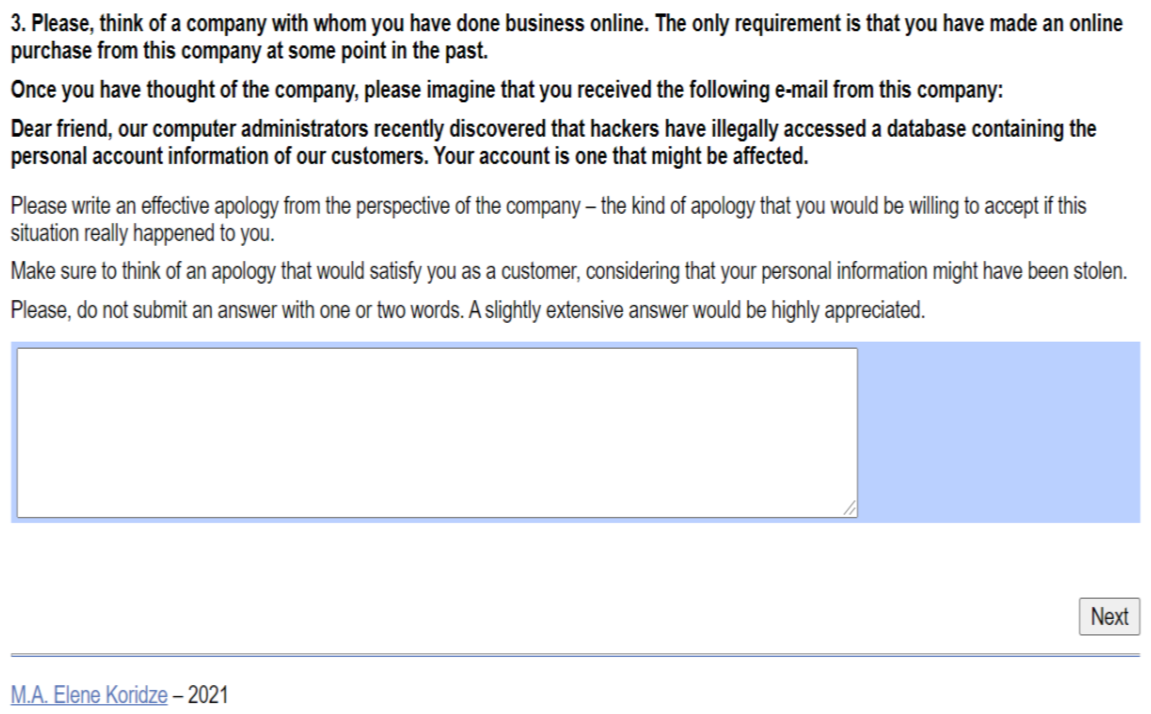
| | never | seldom | sometimes | often | always |
|---|---|---|---|---|---|
| I conduct online transactions | ○ | ○ | ○ | ○ | ○ |

**5. Has your personal information (including bank information) ever been stolen?**

○ yes
○ no

1st scenario – Type of crisis - victim

Source of information - organization



**3. Please, think of a company with whom you have done business online. The only requirement is that you have made an online purchase from this company at some point in the past.**

**Once you have thought of the company, please imagine that you received the following e-mail from this company:**

**Dear friend, our computer administrators recently discovered that hackers have illegally accessed a database containing the personal account information of our customers. Your account is one that might be affected.**

Please write an effective apology from the perspective of the company – the kind of apology that you would be willing to accept if this situation really happened to you.

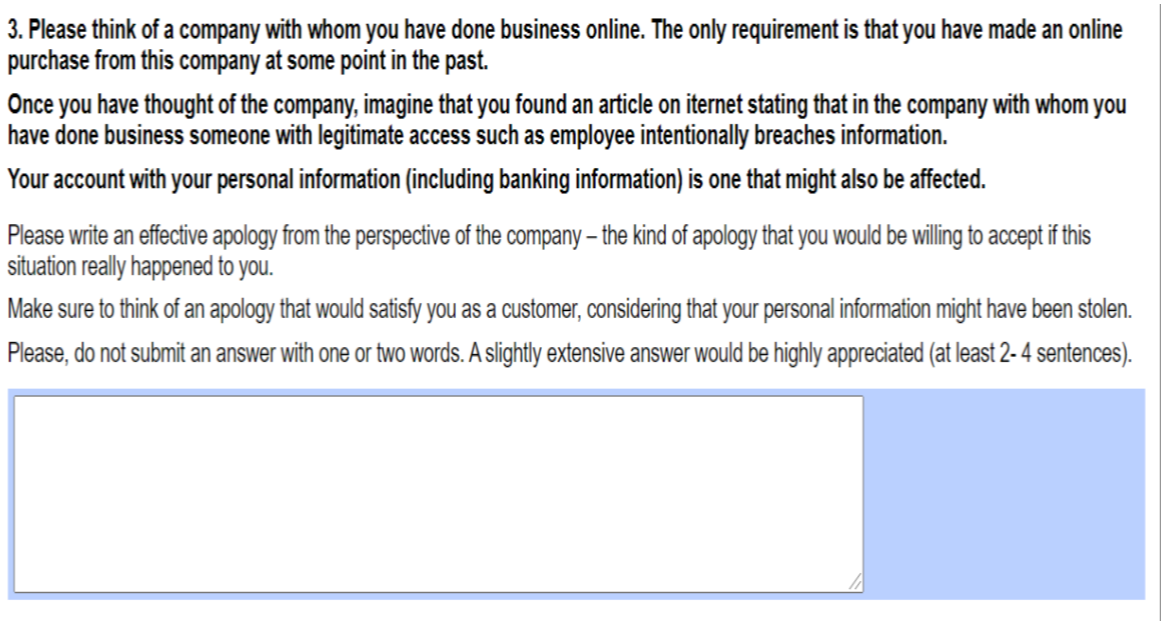
Make sure to think of an apology that would satisfy you as a customer, considering that your personal information might have been stolen.

Please, do not submit an answer with one or two words. A slightly extensive answer would be highly appreciated.

M.A. Elene Koridze – 2021

2nd scenario – Type of crisis – preventable

Source of information – media



**3. Please think of a company with whom you have done business online. The only requirement is that you have made an online purchase from this company at some point in the past.**

**Once you have thought of the company, imagine that you found an article on iternet stating that in the company with whom you have done business someone with legitimate access such as employee intentionally breaches information.**

**Your account with your personal information (including banking information) is one that might also be affected.**

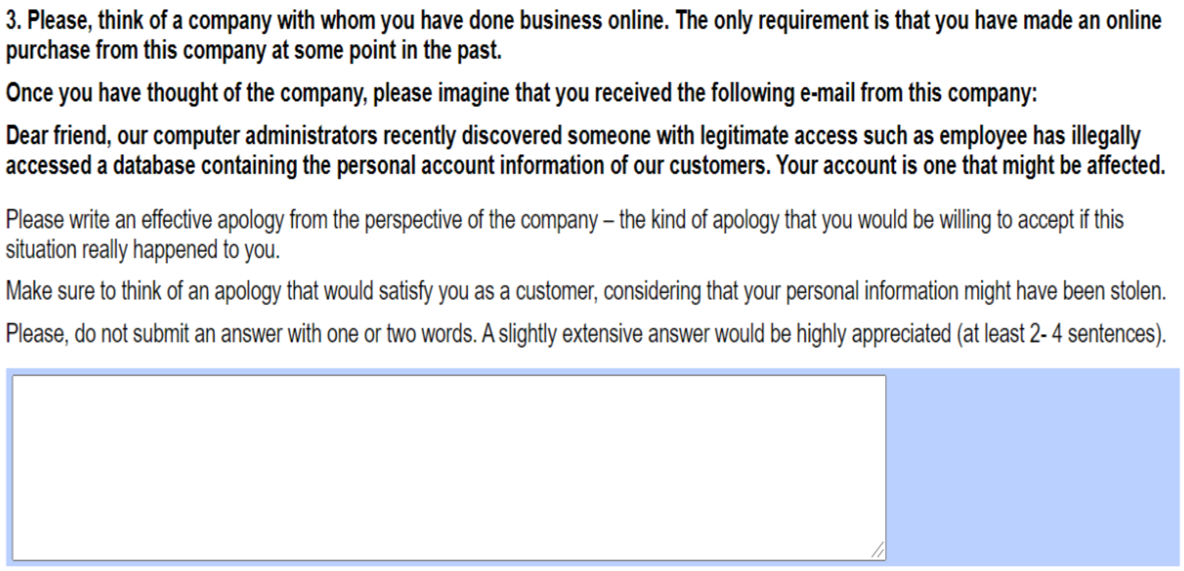
Please write an effective apology from the perspective of the company – the kind of apology that you would be willing to accept if this situation really happened to you.

Make sure to think of an apology that would satisfy you as a customer, considering that your personal information might have been stolen.

Please, do not submit an answer with one or two words. A slightly extensive answer would be highly appreciated (at least 2- 4 sentences).

3rd scenario – Type of crisis - preventable

Source of information - organization



**3. Please, think of a company with whom you have done business online. The only requirement is that you have made an online purchase from this company at some point in the past.**

**Once you have thought of the company, please imagine that you received the following e-mail from this company:**

**Dear friend, our computer administrators recently discovered someone with legitimate access such as employee has illegally accessed a database containing the personal account information of our customers. Your account is one that might be affected.**

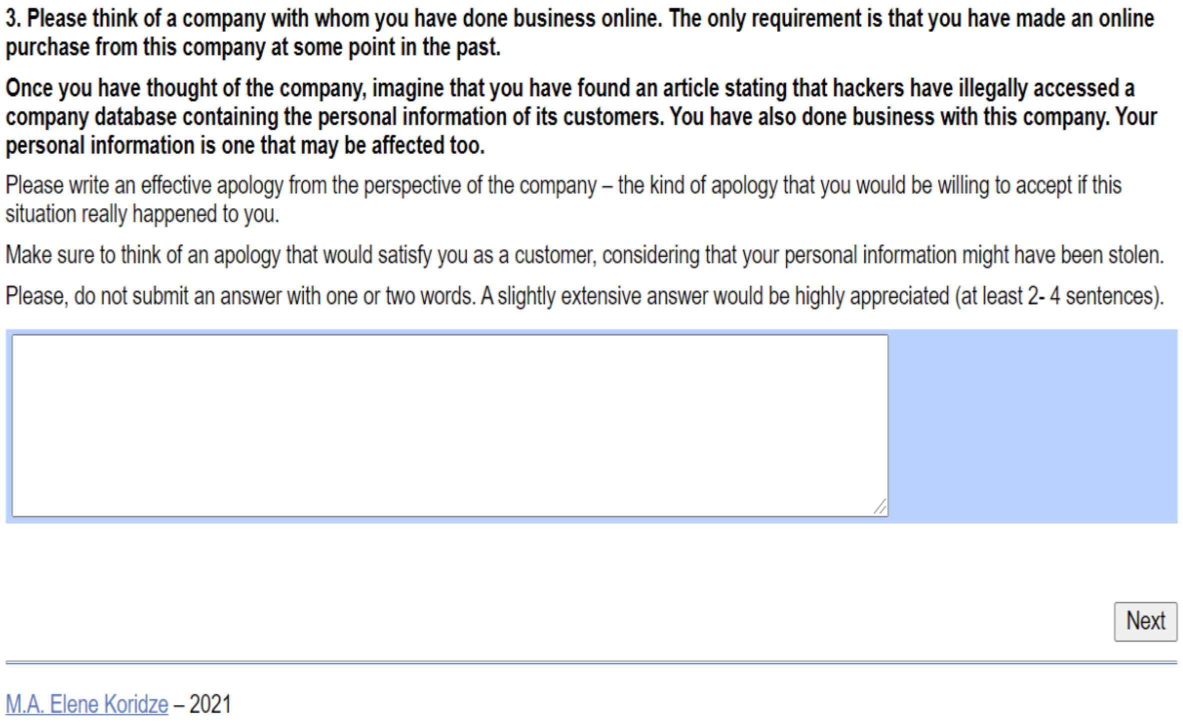
Please write an effective apology from the perspective of the company – the kind of apology that you would be willing to accept if this situation really happened to you.

Make sure to think of an apology that would satisfy you as a customer, considering that your personal information might have been stolen.

Please, do not submit an answer with one or two words. A slightly extensive answer would be highly appreciated (at least 2- 4 sentences).

4th scenario – Type of crisis -victim

Source of information - media



**3. Please think of a company with whom you have done business online. The only requirement is that you have made an online purchase from this company at some point in the past.**

**Once you have thought of the company, imagine that you have found an article stating that hackers have illegally accessed a company database containing the personal information of its customers. You have also done business with this company. Your personal information is one that may be affected too.**

Please write an effective apology from the perspective of the company – the kind of apology that you would be willing to accept if this situation really happened to you.

Make sure to think of an apology that would satisfy you as a customer, considering that your personal information might have been stolen.

Please, do not submit an answer with one or two words. A slightly extensive answer would be highly appreciated (at least 2- 4 sentences).

M.A. Elene Koridze – 2021

## 8 Abstract

The aim of this study is to understand what an appropriate and effective organizational apology is in the preventable and victim organizational crisis from the perspective of a stakeholder. When organizations understand what stakeholders look for in apologies, they may be able to communicate in ways that supports agreement with offended stakeholders. This will help organization to rebuild its´ reputation and restore its ‘social legitimacy. Accordingly, this study analyzed apologies written by stakeholders in a hypothetical crisis scenarios. One hundred participants were asked to write effective apologies in preventable and victim organizational crisis where the source of information about occurred crisis - data breach, was either media or organization itself. The experiment was constructed as a 2X2 factorial design of factors (preventable vs. victim) X (media vs. organization) comparison. Finally, a factorial ANOVA (two – way ANOVA) was conducted to compare main effects of different types of crisis and different types of sources of information on dependent variable – apologies written by stakeholders.

## 9 Abstract (Deutsch)

Das Ziel dieser Studie ist es zu verstehen, was eine angemessene und effektive Entschuldigung (Apology) des Unternehmens in den vermeidbaren und Opferkrisen aus der Perspektive eines Stakeholders ist. Wenn die Organisationen verstehen, wonach Stakeholder in der Entschuldigung suchen, können sie möglicherweise auf eine Weise kommunizieren, die eine Einigung mit beleidigten Stakeholdern unterstützt und die den Ruf der Organisation effektiver repariert und ihre soziale Legitimität wiederherstellt. Dementsprechend, analysierte diese Studie die Entschuldigungen, die von Interessengruppen in den hypothetischen Krisenszenarien geschrieben wurden. Einhundert Teilnehmer wurden erbaten, die wirksame Entschuldigungen für den vermeidbare und Opfer Unternehmenskrisen zu schreiben, bei denen die Informationsquelle über die aufgetretene Krise – die Datenschutzverletzung – entweder die Medien oder die Organisation selbst waren. Das Experiment wurde als faktorielles 2X2 Design aus Faktoren (vermeidbar vs. Opfer) x (Medien vs. Organisation) Vergleich konstruiert. Schließlich, wurde eine faktorielle ANOVA (Zweiwege-ANOVA) durchgeführt, um die Haupteffekte verschiedener Arten von Krisen und verschiedener Arten von Informationsquellen auf abhängige Variablen zu vergleichen – die Entschuldigungen, die von Interessenvertretern geschrieben wurden.