Kurskod: SKDK11
Termin: Vårterminen 2024
Handledare: Rickard Andersson
Examinator: Howard Nofthhaft

A Victim or Not?

A quantitative experimental study of a cyber attack crisis' effect on public attitudes toward an organization and on the organization's reputation

ELLA RYAN & MÄRTA SÖDERBERG

Lunds universitet
Institutionen för strategisk kommunikation

TACK!

Vi vill rikta det största möjliga TACK till vår handledare, Rickard Andersson, för outstanding handledning. Ditt engagemang och stöd ledde oss fram till en uppsats vi både är nöjda med och stolta över. Tack! Vi vill även ta tillfället i akt att tacka er som undervisar på institutionen för strategisk kommunikation vid Lunds universitet för tre lärorika år. Slutligen vill vi tacka varandra för ett fint samarbete och understryka att studien är ett resultat av en likvärdig insats från oss båda.

Ella Ryan & Märta Söderberg

19 maj 2024

Abstract

A Victim or Not?

- *A quantitative experimental study of a cyber attack crisis' effect on public attitudes toward an organization and on the organization's reputation*

This study aims to examine how a cyber attack crisis affects public attitudes toward an organization and the organization's reputation. The study explores the Situational Crisis Communication Theory's (SCCT) victim categorization of a cyber attack crisis in a Swedish context. Further, it examines how individuals' knowledge about cyber attacks, attribution of crisis responsibility, and response strategies affect the public's attitudes and the organization's reputation. By conducting a quantitative experimental survey study, we found that the response strategies *scapegoat* and *victimage* are ineffective in protecting an organization's reputation during a cyber attack crisis and result in worsened attitudes toward the organization. Further, the response strategies *excuse, apology, ingratiation,* and *compensation* were found to have statistically significant positive effects on attitudes toward the organization. These findings contradict the SCCT's framework for crises in the victim cluster. Furthermore, individuals' knowledge about cyber attacks showed minimal impact on public attitudes and the organization's reputation. Attribution of crisis responsibility was found to negatively affect public attitudes toward the organization but has less pronounced effects on the reputation. The study contributes to knowledge in the field of strategic communication and crisis management. Due to the study's findings, we encourage future research to continue exploring the phenomenon of cyber attack crises to contribute with knowledge of how to effectively manage such crises and protect the organization's reputation.

Keywords: crisis communication, SCCT, response strategies, cyber attack, survey experiment.

Numbers of characters including spaces: 97 333

Sammanfattning

Ett offer eller inte?

- *En kvantitativ experimentell studie av en cyberattackkris effekt på allmänhetens attityder gentemot en organisation och organisationens rykte*

Denna studie syftar till att undersöka hur en cyberattackkris påverkar allmänhetens attityder gentemot en organisation samt organisationens rykte. Studien utforskar teorin Situational Crisis Communication Theorys (SCCT) offerkategorisering av en cyberattackkris i en svensk kontext. Vidare undersöks hur individers kunskap om cyberattacker, tillskrivning av krisansvar och nyttjande av olika responsstrategier påverkar allmänhetens attityder och organisationens rykte. Genom att genomföra en kvantitativ experimentell enkätstudie fann vi att responsstrategierna *scapegoat* och *victimage* var ineffektiva för att skydda organisationens rykte under en cyberattackkris och resulterade i försämrade attityder gentemot organisationen. Därtill visade sig responsstrategierna *excuse*, *apology*, *ingratiation* och *compensation* ha statistiskt signifikanta positiva effekter på allmänhetens attityd gentemot organisationen. Dessa resultat står i motsats och skiljer sig från SCCTs ramverk för kriser i offerkategorin. Dessutom visade individers kunskap om cyberattacker ha en minimal påverkan på attityden mot organisationen såväl som dess rykte. Tillskrivningen av krisansvar visa sig påverka allmänhetens attityder gentemot organisationen negativ men inte organisationens rykte. Studien bidrar med kunskap inom forskningsfälten strategisk kommunikation och crisis management. Med studiens resultat i åtanke uppmanar vi framtida forskning att fortsätta utforska fenomenet cyberattackskriser för att bidra med kunskap om hur man effektivt hanterar en sådan kris har för att skydda organisationens rykte.

Nyckelord: kriskommunikation, SCCT, responsstrategier, cyberattack, enkätexperiment

Antal tecken inklusive blanksteg: 97 333

Table of contents

1. Introduction

"The secret in crisis management is not good vs. bad, it's preventing the bad from getting worse." - Andy Gilman

Organizations' reputations are widely acknowledged as a valuable asset (Rosenbaum-Elliot, Percy, Pervan, 2015; Zerfass & Viertmann, 2017; Winkelman, 1999). Crises pose a threat to damage an organization's reputation (Coombs, 2015) and can lead to negative public attitudes toward the organization (Krishna and Vibber, 2017). Globalization and technological development have resulted in complex societies. Increased complexity can enhance experiences of increased numbers of crises and the emergence of new crisis types (Frandsen & Johansen, 2017). In recent years, cyber attacks against organizations have been reported more frequently (IBM, 2023). As the number of cyber attacks increases, so do organizations' fear of falling victim of an attack.

In the research field of crisis management, the Situational Crisis Communication Theory (SCCT) by Timothy W. Coombs is one of the most prominent theories which provides an evidence-based framework based on experimental methods (Frandsen & Johansen, 2017). The framework offers guidance for management of specific crisis types and for protection of an organization's reputation (Coombs, 2007; 2015). The organization needs to communicate with its stakeholders to mitigate reputational damage caused by a crisis (Frandsen & Johansen, 2017). SCCT provides a detailed framework with several response strategies that are matched to specific types of crises and situations (Coombs, 2015). SCCT suggests that the public is likely to perceive the targeted organization as a *victim* when it is subjected to a cyber attack since a malicious act by an external actor makes the organization a victim (Brown & Ki, 2013; Coombs, 2015; Krishna & Vibber, 2017). Being a victim means minimal a*ttribution of crisis responsibility* for the organization. Consequently, there is a minimal effect on the organization's reputation (Coombs, 2015).

However, contemporary societal shifts and recent research indicate that the public perceptions of organizations subjected to a cyber attack may not align with Coombs' (2015) *victim* categorization. Krishna and Vibber (2017) found that the public's response to an organization subjected to a cyber attack that employed a *victimage* response strategy largely contradicted the assumptions of SCCT's victim cluster. Further, damage to an organization's reputation following a cyber attack has been shown to negatively influence market shares (Roškot, Wanasika, & Kreckova Kroupova, 2021) and consumers' purchase intentions (Wahab, Khan, Kamontip, Hussain, & Amir, 2023).

Awareness of cyber attacks and cyber security is becoming common knowledge among the public in Sweden. The increase in attacks has led to governmental establishments for cyber security and new authorities (Myndigheten för samhällsskydd och beredskap, 2024). Additionally, educational programs at workplaces are implemented to raise awareness about cyber security. Based on this, the Swedish public's expectations for organizations to withstand cyber attacks are likely to increase. This is because individuals tend to be more skeptical of events within frames of their knowledge (Jallinoja & Aro, 2000). In turn, skepticism influences consumers' attitudes toward an organization (Romani, Grappi & Bagozzi, 2016; Bae, 2018).

Cyber attacks seem to create a new context and a new crisis type where the organization is subjected to malicious acts but still not perceived as a victim by the public. This raises new demands and navigations for organizations' crisis management. Furthermore, cyber attacks is a relatively new phenomenon. Thus, there is limited research and knowledge about the crisis type and how it affects the public's attitude toward the organization and the organizational reputation (Krishna & Vibber, 2017; Wahab, et al., 2023). To contribute with knowledge about this new type of crisis, the present thesis aims to examine the public attitudes toward an organization subjected to a cyber attack and analyze a cyber attack's impact on organizational reputation.

1.2 Problematization

According to SCCT, if an external agent causes damage leading to a public crisis, the impact on the organization's reputation will be minimal since the crisis was not caused by the organization itself. Consequently, the public will attribute minimal crisis responsibility to the organization, making such crises belong to the *victim cluster* (Coombs, 2015). Given that background, we argue that cyber attack crises belong in the victim cluster along with other crises such as e.g.

product tampering. However, societal shifts and previous research indicate that public perceptions of cyber attack crises do not align with this categorization (Coombs, 2015). Previous research notes that cyber attacks pose a great threat to reputational damage and can lead to a negative attitude towards the organization by the public even though it is a malicious act performed by a hostile external actor (Krishna & Vibber 2017; Kuiper & Schonheit, 2022; Wahab et al., 2023).

SCCT posits that by identifying what type of crisis the organization is subjected to the crisis manager can anticipate the level of reputational threat the crisis will cause and employ an appropriate response strategy (Coombs & Holladay, 1996; Coombs, 2015). However, suppose the crisis manager follows SCCT and perceives a cyber attack crisis as low risk for reputational damage, categorizing the organization as a victim, while the public considers the crisis as preventable by the organization. In that case, it may lead to a mismanagement of the crisis and result in a double crisis. A double crisis occurs when a communication crisis coincides with the primary crisis to the extent that the organization in crisis cannot effectively manage the communication essential for addressing the original crisis (Johansen & Frandsen, 2007).

Based on the fact a cyber attack crisis can represent a new type of crisis, deviating from the well-established framework provided by the SCCT, we believe this phenomenon requires further investigation to develop an expanded understanding. From the perspective of strategic communication, it is valuable to explore this area, because strategic communication "*encompasses all communication that is substantial for the survival and sustained success of an entity. Specifically, strategic communication is the purposeful use of communication by an entity to engage in conversations of strategic significance to its goals"* (Zerfass, Verčič, Nothhaft & Werder, 2018, p. 487).

Despite extensive research within the research fields of crisis communication and public relations, we argue that we have identified a knowledge gap for cyber attacks and how these crises affect public attitudes toward an organization and its organizational reputation. There is a limited amount of scholarly research from various research fields that explore cyber attacks' impact on an organization. The available research within the fields of crisis management and public relations predominantly originates from the US and is based on American cases. We have not found any research utilizing SCCT in its experimental evidence-based original form, examining the effectiveness of response strategies to protect organizational reputation in the

context of cyber attacks which this study aims to do. Additionally, few studies overall examine the SCCT in real settings, measuring the public's attitudes to real life and current problems (Krishna & Vibber, 2017).

1.3 Aim and research questions

This study aims to examine cyber attack crises' effect on public attitudes toward organizations and organizations' reputations. Specifically, the study aims to examine if knowledge about cyber attacks, attribution of crisis responsibility, and different response strategies affect the public's attitudes toward an organization and the organization's reputation in the context of a cyber attack crisis. By conducting a quantitative experimental survey study, we aim to identify what response strategies provided by SCCT result in a positive attitude toward an organization and a stronger organizational reputation.

The study contributes with knowledge within the research fields of crisis management, public relations, and strategic communication. Likewise, the result of the study can provide insights for practitioners to make informed decisions to achieve more strategic communication when managing a cyber attack crisis. To reach the aim of the study, the following research questions have been formulated.

RQ1: *Does an individual's knowledge of cyber attacks influence the attitudes toward an organization and the organization's reputation during a cyber attack crisis?*

RQ2a: *How does attribution of crisis responsibility impact the attitudes toward an organization and the organization's reputation when subjected to a cyber attack?*

RQ2b: *To what extent does the public attribute crisis responsibility to an organization subjected to a cyber attack?*

RQ3: *What response strategies have positive effects on organizational reputation and attitudes toward an organization when an organization has been subjected to a cyber attack crisis?*

RQ4: *Is an organization subjected to a cyber attack perceived by the public in line with the victim crisis frame of Coomb's Situational Crisis Communication Theory?*

1.4 Limitations

The thesis is rooted in the research field of strategic communication with a focus on crisis communication following SCCT. We have chosen to limit the scope of our research to examine the initial phase of a cyber attack crisis. The three factors, knowledge, attribution of crisis responsibility, and response strategies are examined. Thus, the entirety of SCCT, which also takes into account the organization's performance history (Coombs, 2015), is not examined. Furthermore, the study does not analyze stakeholders' interactions with the organization, which additionally shapes narratives and consequently can affect reputation (Frandsen & Johansen, 2017). The scenario presented in this thesis is limited to one type of crisis, a cyber attack, and three responses to mitigate the effects of that crisis. Lastly, the study was conducted in a Swedish context which consequently should be considered to the study's results and conclusions.

1.5 Definitions of keywords and concepts

1.5.1 Crisis

There are numerous definitions of the word 'crisis' (Frandsen & Johansen, 2017). For this study, the authors have adopted a definition and understanding provided by Coombs (2015) since the study's theoretical framework is based on his SCCT. He argues that *"A crisis is the perception of an unpredictable event that threatens important expectancies of stakeholders related health, safety, environmental, and economic issues, and can seriously impact an organization's performance and generate negative outcome."* (Coombs, 2015, p. 3).

1.5.2 Crisis responsibility

Crisis responsibility represents the degree to which stakeholders blame the organization for the crisis event. Furthermore, as perceptions of crisis responsibility strengthen, the threat of reputational damage increases (Coombs, 2015).

1.5.3 Cyber attack crisis

According to IBM, a cyber attack is *"... any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device."* (IBM, n.d). In this study, we have adopted this quite broad umbrella

definition, however, we acknowledge that there exist more specified technical formulations and descriptions depending on the aim and design of the attack.

1.5.4 Organizational reputation

There are several definitions of the concept of *organizational reputation*. Organizational reputation can be interpreted as awareness, an assessment, or an asset (Frandsen & Johansen, 2017; Fombrun, 2012). We interpret the concept as a collective assessment of an organization's attractiveness, which is an asset, to certain stakeholder groups compared to other organizations' attractiveness. In this thesis, the expressions "organizational reputation" and "organization's reputation" have the same meaning.

2. Previous research

In the following section, a literature review of relevant previous research for the study is presented. The literature review was systematically conducted and a snowball effect was utilized. Keywords for the searches were: organizational reputation, attitudes, crisis management, knowledge affecting attitudes, and cyber attacks crisis management.

Most research within the fields of crisis communication and public relations originates from America and is based on American cases. Even though this study does not aim to examine cultural differences we want to emphasize the need to explore the phenomena of cyber attacks crisis in different cultural contexts. Our ambition with this study is to provide as nuanced previous research as possible, thus we have actively sought previous research from different geographical areas. Furthermore, this thesis will contribute to the field from a Swedish perspective.

2.1 Organizational reputation

Coombs (2007) declares that reputation is a valuable and intangible asset. He argues that a favorable organizational reputation can attract different stakeholder groups, generate investment interest, and improve financial performance. Moreover, he notes that reputation encompasses stakeholders' overall assessment of how an organization fulfills its expectations, considering past behaviors and all kinds of information they have received about the organization. This assessment also involves comparing the organization's behavior to general expectations regarding how an organization should behave. Crises and the cause of a crisis thus pose a threat to damage an organization’s reputation since it can affect stakeholders' assessment of the organization (Coombs & Holladay, 2002).

A closely related concept to organizational reputation is *imag*e which, as well, is a multi-defined conception (Gray & Balmer, 1998). The two predominant views are the *projected*

image (how insiders want outsiders to see the organization) and the *perceived image* (how outsiders indeed perceive the organization) (Frandsen & Johansen, 2017). Our understanding of the concept of image aligns with the latter one. The question then arises regarding what differentiates the concepts of image and organizational reputation. Frandsen and Johansen (2017) state that scholars with our interpretation of the two concepts must define them as long as they don't consider them synonyms.

Our understanding of the concepts of reputation and image largely overlaps. They both refer to the public's perception of the organization. In previous research, they commonly appear mixed and as synonyms (Frandsen & Johansen, 2017). Reputation is attitudes formed through a long-term evaluation of the organization (Coombs, 2015) meanwhile image is more of an instant perception (Gray & Balmer, 1998). The understanding of reputation as something constructed from a long-term relationship, including history and multiple interactions could conflict with the study's experimental research design of a fictitious organization. However, given the well-established theoretical framework SCCT that serves as the foundation for this thesis, along with its utilization of similar empirical data collection methods and references to reputation (Coombs, 2015), we have opted to adhere to the terminology of organizational reputation.

2.2 Cyber attacks as a reputational threat

As mentioned in the introduction and problematization, cyber attack crises provide a new context that organizations and crisis managers need to navigate. Informed by SCCT, a crisis caused by malevolent acts against an organization, making the organization a victim itself, belongs to the victim cluster. Therefore, according to the theory, an organization should be attributed with none or minimal crisis responsibility resulting in a minimal reputational threat (Coomb, 2007; 2015). As recently as a decade ago, Brown and Ki (2013) listed organizations subjected to cyber attacks as an example of a crisis in the victim cluster.

However, more recent research indicates a shift in the public's perception of crises caused by cyber attacks. Krishna & Vibber (2017) revealed that the public's reaction on social media toward Sony was strongly negative after the cooperation was subjected to a cyber attack. Additionally, they concluded that the organizational reputational damage from such a crisis largely contradicted SCCT's assumptions about victim cluster crises. Wahab et al. (2023) examined the impact of cyber attacks on consumer behavioral intentions for online purchases.

Their findings revealed that a cyber attack in the organization's crisis history had a largely negative effect on behavioral intentions.

Further evidence for the claim that cyber attacks should be understood as a new type of crisis is Wang and Park's (2017) introduction of a new public communication model for how organizations should manage their external stakeholders during a data breach to protect the organization's reputation. The article was published in Issues in Information Systems and the scholar has a background in information communication technology. Wang and Park (2017) advocate for using SCCT response strategies but add the aspect of time. Regardless, a negative impact on the company's reputation and market value was identified. Wang and Johnson (2018) developed the model and further examined the scapegoating strategy which was found to be ineffective.

Kuipers and Schonheit (2022) analyzed organizations' communication and reputational damage for 64 cases of cyber attack situations. The authors found that admitting responsibility was beneficial and that denial strategies damaged the organizational reputation. Moreover, organizations that adhered to and focused on a single response strategy throughout their communication outperformed those that inconsistently mixed different strategies. Consistent and immediate implementation of the rebuild strategies *compensation* and *apology* combined with bolstering strategy *ingratiation,* improved reputational recovery from the crisis. Additionally, self-disclosure enabled companies to exert a positive influence on media coverage (Kuipers & Schonheit, 2022).

2.3 Attitudes toward an organization

Lafferty and Goldsmith (2005) explain that attitudes are feelings centered or directed at an object. Further, the scholars state that attitudes are evaluative by nature, implying a level of attribution of goodness or badness toward the object of the attitude. Attitudes affect and shape behaviors such as purchase intentions (Wahab et al., 2023) and the willingness to engage in new contexts (Raju, Lonial & Mangold, 1995).

The concepts of organizational reputation (see *2.1 Organizational Reputation*) and attitudes toward an organization are related but differ in scope and focus similar to image and reputation. Reputation is also attitudinal, however, reputation refers to an overall perception or evaluation of an organization by stakeholders and constructed over time through interactions

with the organization (Coombs & Holladay, 2002; Frandsen & Johansen, 2017). In comparison, attitudes toward an organization refer to an individual's internal evaluation of the organization (Lafferty & Goldsmith, 2005). Thus, attitudes reflect the individual's subjective perception of an organization based on their impression. Ones attitude towards an organization is a posture of a feeling that ethier can be positive, negative, or neutral. It is influenced by factors such as the individual's personal values, experience, and expectations (Spears & Singh, 2004).

In summary, while reputation encompasses the overall perception of an organization, attitudes toward an organization focus on individuals' specific feelings and evaluations of that organization. Attitudes contribute to the formation and maintenance of an organization's reputation, but reputation extends beyond individual attitudes to represent the total public perception of the organization within its environment. Based on this, we argue that attitudes toward an organization are relevant and act as a good complement to organizational reputation in the study and thus both concepts are represented in the study's model.

2.4 Knowledge affecting attitudes

Friestad & Wright (1994) assert that an individual's knowledge about a certain topic ze's attitude. Further, an individual's primary response when exposed to new information is to form an attitude toward both the topic and the sender of the information. Attitudes are formed and motivated by the need to understand the cause of a message or situation (Friestad & Wright, 1994). This process is referred to as sense-making (Weick, 1988). The previously mentioned factors will in turn influence an individual's attitudes. Raju et al., (1995) argue that the feeling of knowing, subjective knowledge, has a prominent effect in a decision process. Their study's results closely correlate high subjective knowledge with high trust and confidence as affecting decisions.

The concept of *skepticism* refers to an individual's bias to distrust or disbelieve. The concept is related to the *Attribution Theory* as it influences consumers' perceptions and behaviors toward an organization (Romani et al., 2016; Bae, 2018). For this thesis, *situational skepticism* provides a frame as it is understood as a state that varies depending on the context not as a personality trait. Skepticism is thus related to the perception of specific actions or information communicated by the organization. Individuals employ their knowledge and information to interpret and evaluate these actions and pieces of information, resulting in the emergence of skepticism in some cases which affects ze's evaluation and attitudes (Romani et al., 2016).

Jallinoja & Aro's (2000) study provided a basis for the evident association between knowledge and attitudes. Individuals with high knowledge were found to be less prone to accept information they sought to be ambiguous, demanding comprehensive information to assess a situation. Additionally, high knowledge proved to result in a higher degree of skepticism.

Downs, Holbrook and Cranor (2007) conducted a study to provide a better understanding of which factors influence individuals' tendency to succumb to the cyber attack method phishing. The results indicated that individuals with higher knowledge were less prone to click on unknown links and thus fall for the attack. Knowledge and expertise were found to be predictors of behavioral responses which are affected by attitudes.

2.5 Crisis management to protect organizational reputation

As previously mentioned, crises pose a threat to an organization's reputation. Therefore, one of the main objectives of crisis management is to protect and repair the reputation of an organization during and after a crisis (Allen & Caillouet, 1994; Frandsen & Johansen, 2017). Crisis managers aim to protect the positive aspects of an organization's reputation and prevent the negative associations generated by a crisis from corrupting the public's view of the organization (Coombs, 2015). Coombs and Holladay (2002) assert communication as the factor that shapes stakeholders' perception of a crisis and the organization involved in the crisis.

Ma and Zhan (2016) proved a negative correlation between an organization's crisis responsibility and its reputation. Experimental studies have demonstrated an increase in reputational damage as the public attributes higher responsibility to the organization for a crisis (Coombs & Holladay, 2002). Crises understood as preventable by the public was proven to cause the most reputational damage (Claeys, Cauberghe, & Vyncke, 2010; Verhoeven, Van Hoof, Ter Keurs, & Van Vuuren, 2012).

Crisis management is described to be a process of predicting possible crises, identifying crises, and managing crises by applying proper strategies to avert or mitigate the incident. (Mitroff & Pearson, 1993; Sahin, Ulubeyli & Kazaza, 2015). Further, the importance of an organization's crisis preparedness is pivotal in its aim to manage the situation effectively and with the lowest possible damage and disruptions to the organization and its operations (Paraskevas, 2006; Coombs, 2015). Sahin et al. (2015) and Mikušová and Horvathova (2019) emphasize the implementation of proper strategies and processes throughout the organization to

enable both efficiency and flexibility when navigating a crisis. By preparing the organization with proper strategies and frameworks, the initial burden on the crisis management team to assess and respond eases as they take on the crisis (Sahin et al., 2015; Mikušová & Horvathova, 2019).

New perspectives within the fields of strategic communication and crisis management criticize researchers and practitioners who preach about the importance of comprehensive crisis plans. Falkheimer and Heide (2022) argue that many organizations today excessively place their faith in the feeling of having a crisis plan in place meaning that it can lead to a false sense of security, and prolonged reactions and decisions in the organization. They highlight the importance of flexibility in managing crises advocating for *strategic improvisation.* We acknowledge this emerging perspective, however, we believe that there is a need for clear frameworks based on theory to support crisis-managing practitioners' work.

3. Theoretical framework

In the following chapter, the study's theoretical framework is presented. This study explores the Situational Crisis Communication Theory (SCCT) by Coombs (1995; 1998; 2007; 2015) in a cyber attack context. First, the theory is presented in its entirety, followed by a deeper explanation of the two components, attribution of crisis responsibility and response strategies. Lastly, the study's hypotheses, which aim to contribute to answering the research questions, are presented and visualized in a model.

3.1 Situational Crisis Communication Theory (SCCT)

SCCT provides a comprehensive framework for crisis managers on how to manage crises and protect an organization's reputation. SCCT posits that by understanding the crisis type and the organization's situation, the crisis manager can anticipate the potential risk it poses to the reputation and thus choose an appropriate response strategy to manage the crisis and protect the organization's reputation (Coombs, 2015). The key components in the theory consist of *crisis type, attribution of crisis responsibility, crisis history, prior relational reputation,* and *response strategies* which affect organizational reputation and behavioral intentions (see *Figure 1*).

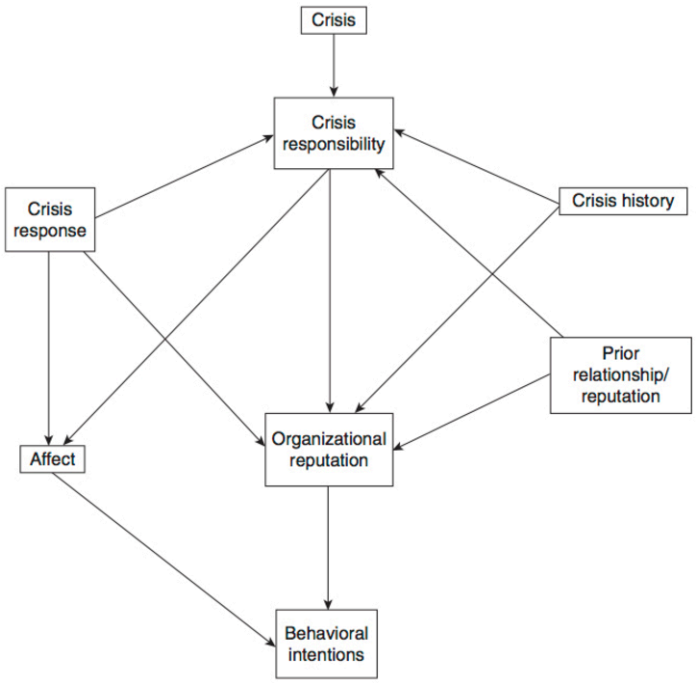

Figure 1: The Situational Crisis Communication Theory (SCCT) (Coombs, 2015).

Depending on the crisis type, the amount of attributed crisis responsibility to the organization differs. The higher the attribution of crisis responsibility toward the organization, the greater the reputational threat and vice versa (Coombs, 2007). The reputational threat is constituted by the amount of damage the crisis could inflict if no action is taken (Coombs, 2015).

SCCT gathers different crisis types into three crisis clusters depending on the level of attributed crisis responsibility (see *Figure 2*). By understanding the crisis type and the crisis responsibility attributed the crisis manager can determine which crisis response strategies will be suitable to employ to protect the reputation (Coombs, 2007).

Cluster	Crisis types examples	Attribution of crisis responsibility	Reputational threat
Victim	• Natural disaster: Acts of nature damage an organization such as an earthquake. • Rumor: False and damaging information about an organization is being circulated. • Product tampering/Malevolence: External agent causes damage to an organization.	In these crisis types, the organization is also a victim of the crisis. The attribution of crisis responsibility is weak/minimal.	No or minimal reputational threat.
Accidental	• Challenges: Stakeholders claim an organization is operating in an inappropriate manner. • Technical-error accidents: A technology or equipment failure causes an industrial accident. • Technical-error product harm: A technology or equipment failure causes a product to be recalled	In these crisis types, the organizational actions leading to the crisis were unintentional. The attributions of crisis responsibility is low to medium.	Moderate reputational threat.
Preventable	• Human-error accidents: Human error causes an industrial accident. • Human-error product harm: Human error causes a product to be recalled. • Organizational misdeed with no injuries: Stakeholders are deceived without injury. • Organizational misdeed management misconduct: Laws or regulations are violated by management. • Organizational misdeed with injuries: Stakeholders are placed at risk by management and injuries occur.	In these crisis types, the organization knowingly placed people at risk, took inappropriate actions or violated a law/regulations. The attribution of crisis responsibility high/strong.	Severe reputational threat.

Figure 2. SCCT crisis types in crisis clusters.

SCCT takes into account an organization's crisis history and prior relational reputation i.e. the organization's performance history (Coombs, 2007). Crisis history refers to whether an organization has had a similar crisis in the past. Prior relational reputation refers to how well, or unwell, an organization has treated its public in other contexts. An unfavorable prior relational reputation implies the organization has little consideration for its public. An unfavorable performance history intensifies the attributions of crisis responsibility and thus increases the reputational threat when a new crisis occurs (Coombs, 2015). Kuipers and Schonheit, (2022) found that crisis history did not have any significant effect when the crisis was caused by a cyber attack. Coombs and Holladay (2002) analyzed performance history's effect on the organizational reputation in crisis with no significant results between neutral and favorable. Due to limited resources and the results of their study, we have decided to not include these variables in the study's model. Therefore, this study alludes to a scenario where the organizations in question have a good or neutral performance history. Consequently, the results of this study will only apply to such scenarios.

3.1.1 Attribution of crisis responsibility toward an organization

SCCT has its roots in the *Attribution Theory* which posits that stakeholders strive to find the cause of an event, especially in negative and unexpected situations (Coombs, 2007). Crisis responsibility is constituted by how much stakeholders believe internal organizational actions caused the crisis. The responsibility is based on the proportion of the factors locus, stability, and controllability (McAuley, Duncan & Russel, 1992; Coombs & Holladay, 1996). Internal

attributions of the factors create a situation in which the perception is that the organization is responsible and the opposite if the attributions are external (Coombs, 1995).

Studies by Weiner, Graham & Chandler (1982) provide a basis for emotional influence on attributing responsibility. They explain how stakeholders react with sympathy towards the one they perceive to be a victim but with anger towards the one they perceive as a blameworthy victim.

3.1.2 Response strategies

To manage the effects of the crisis SCCT provides a framework of response strategies to help crisis managers handle the situation. The *Attribution Theory* acted as a theoretical ground for the response strategies (Coombs, 2007). Three groups form the primary response strategies of SCCT *denial*, *diminish,* and *rebuild*. SCCT separates crisis response strategies from instructing information. Instructing information represents what stakeholders need and want to know after a crisis hits and should always be included in a response (Coombs, 2006).

Deny strategies seek to erase the connection between the organization and the crisis and are best utilized in rumor and challenge crises.

Diminishing strategies argue the severity of the crisis is not as bad as stakeholders think or that the crisis was out of the organization's control. By mitigating the organization's connection or the stakeholder's view of the situation the negative effects are reduced. Diminish strategies are appropriate for accidental crises with low responsibility attributions (Coombs, 2006).

Rebuild strategies are a tool for generating new organizational assets by attempting to improve the organization's reputation. Offering material or symbolic gestures of compensation to the victims, by doing so the organization is benefitting the stakeholders which is seen as positive and negates the negative of the crisis (Coombs, 2006). Rebuild strategies are recommended for preventable crises with strong responsibility attributions.

Additionally, bolstering strategies can be combined with any other strategy. *Victimage* is suitable for crisis types such as workplace violence, product tampering, cyber attacks, natural disasters, and rumors (Brown & Ki, 2013). *Reminder* and *ingratiation* is used to reinforce positive perceptions of the organization and to maintain or improve relationships with stakeholders. See *Figure 3* for further explanations.

Deny	Diminish	Rebuild	Bolstering
• Attack the accuser: Crisis manager confronts the person or group claiming something is wrong with the organization. • Denial: Crisis manager asserts that there is no crisis. • Scapegoat: Crisis manager blames some person or group outside of the organization for the crisis.	• Excuse: Crisis manager minimizes organizational responsibility by denying intent to do harm and/or claiming inability to control the events that triggered the crisis. • Justification: Crisis manager minimizes the perceived damage caused by the crisis.	• Compensation: Crisis manager offers money or other gifts to victims. • Apology: Crisis manager indicates the organization takes full responsibility for the crisis and ask stakeholders for forgiveness.	• Reminder: Tell stakeholders about the past good works of the organization. • Ingratiation: Crisis manager praises stakeholders and/or reminds them of past good works by the organization. • Victimage: Crisis managers remind stakeholders that the organization is a victim of the crisis too.

Figure 3. SCCT response strategies.

3.2 Application of theory

Informed by previous research and the SCCT the following five hypotheses were formulated to reach the study's aim and to operationalize the study's research questions.

H1a: *High knowledge of cyber attacks will have negative effects on individual's attitude toward the organization when the organization is subjected to a cyber attack crisis.*

H1b: *High knowledge of cyber attacks will have negative effects on individuals' perceptions of the organization's reputation when the organization is subjected to a cyber attack crisis*

H2a: *High attribution of crisis responsibility will have negative effects on attitudes toward the organization.*

H2b: *High attribution of crisis responsibility will have negative effects on the organization's reputation.*

H3a: *Applying scapegoat and victimage response strategies when managing a cyber attack crisis will have negative effects on attitude towards an organization.*

H3b: *Applying scapegoat and victimage response strategies when managing a cyber attack crisis will result in a weaker organizational reputation than other response strategies.*

H4a: *Applying an excuse response strategy when managing a cyber attack crisis will have positive effects on attitudes toward an organization.*

H4b: *Applying an excuse response strategy when managing a cyber attack crisis will result in a stronger organizational reputation than scapegoat and victimage response strategies.*

H5a: *Applying rebuild response strategies when managing a cyber attack crisis will have positive effects on attitudes toward an organization.*

H5b: *Applying rebuild response strategies when managing a cyber attack crisis will result in a stronger organizational reputation than scapegoat and victimage response strategies.*

To visualize the study's hypotheses the following theoretical model was constructed.

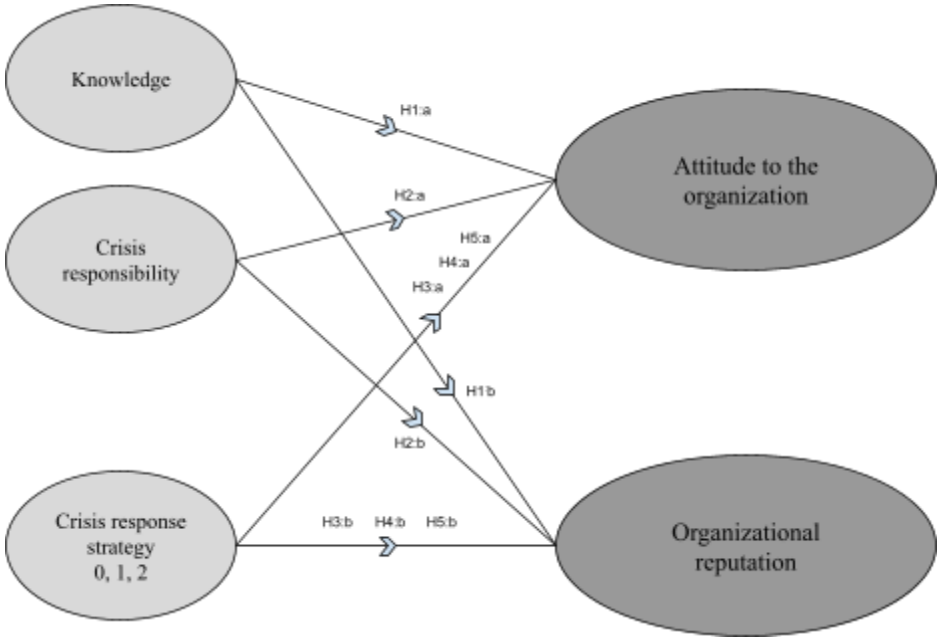

Figure 4. The study's model - visualizations of the hypotheses.

4. Method

In this chapter, the methodology upon which the study is based is discussed. First, the scientific approach and research method are presented followed by the sampling method. The method for collecting empirical data, a digital survey experiment, is discussed and explained. We also outline the experimental conditions in the form of stimuli in detail. Furthermore, the study's dependent and independent variables, along with measurement scales, are presented followed by a report on the data analysis methods and procedures. The chapter concludes with a reflection on the methodology and the study's applicability

4.1 Scientific approach

The study's scientific approach is grounded in empirical scientific theory with a post-positivist perspective. Our epistemological stance suggests that knowledge can be acquired and substantiated through observations of reality. As a result, we as researchers maintain a more neutral stance toward the research subject (Djurfeldt, Larsson & Stjärnhagen, 2018). What differs between a post-positivistic research approach compared to classic positivistic, is the assumptions of the existence of an objective reality of a research problem (Craig & Muller, 2007). The post-positivist approach rejects certain assumptions from a strict positivist epistemology and acknowledges the influence of human subjectivity and biases in research. Moreover, post-positivism advocates for a more nuanced understanding of reality and the inclusion of multiple perspectives in a research process (Craig & Muller, 2007). Ryan (2006) states that post-positivist social researchers assume more of a learning role than a testing one.

The study was conducted with a deductive approach with the aim of testing theory. In deductive research, the researcher(s) formulate hypotheses based on previous research and theories that indicate the predicted outcome of the study's results (Gustafsson & Holmberg, 2023). The hypotheses will either be confirmed or rejected in the study's analysis depending on whether a statistically significant relationship is found.

4.2 Research method

The research method for this study was quantitative. Rousseau (2006) argues that research should be supported by scientific evidence from empirical research rather than personal preference and unscientific experiences. Through the observations of reality, we aim to collect experiences that reveal a specific pattern that can be explained and validated through quantitative methods (Gustafsson & Holmberg, 2023).

Related to the aim of the study, we aim to collect and assess data as objectively as possible to obtain knowledge about the phenomenon of cyber attack crises' impact on public attitude toward the organization and organizational reputation. The study's hypotheses were formulated based on previous research and the study's framework, indicating the predicted outcome of the study's results.

4.3 Sampling

A sample is defined as a number of individuals pertaining to a, for the study, relevant group. In a quantitative study, the sample is the basis to be able to provide reliable and generalizable conclusions about the topic and the target population. Therefore, a sample that constitutes a representative depiction of the overall population is preferable (Boyle & Schmierbach, 2015). Due to limited resources, a nonrandom convenience sampling method was utilized. The method is well-adapted for studies of this magnitude (Trost & Hultåker, 2016). Furthermore, the survey had a delimitation in ages younger than age 18, a decision primarily based on ethical reasons. As some research argues, experimental methods are inclined to inflict psychological stress, especially among young participants (Boyle & Schmierbach, 2015). An upper age limit was implemented due to the inability to research the target group effectively due to limited resources. The target group consisted of individuals aged 18-69, residing in Sweden, and who were aware of the phenomenon of cyber attacks. Conclusively the study had a total of 121 respondents, 115 constituted the final sample. The sample consisted of 81 women and 34 men.

4.4 Data collection

We aim to examine how knowledge, attribution of crisis responsibility, and a number of response strategies affect attitudes toward an organization and the organizational reputation in a cyber

attack crisis context. The data collection for the study was carried out through a digital survey experiment.

We considered a digital survey the most convenient method to collect data for the study given it is an agile and time-effective way to reach participants. Bryman & Bell (2017) claim that collecting data through a digital survey minimizes the risk of error in the data as the data collected is automatically and systematically transferred to an Excel-sheet. Further, a digital survey experiment is an advantageous method when one aims to examine how different factors affect variations in attitudes (Gustafsson and Holmberg, 2023). Since this study aims to examine what response strategies have positive effects on the public's attitudes toward an organization and an organization's reputation when subjected to a cyber attack crisis we found this method suitable.

The survey was distributed through social media e.g. LinkedIn, Facebook, and Instagram. The survey was opened for respondents to enter for two weeks, 2024-04-22 to 2024-05-06.

4.4.1 Experiment

As stated previously, the study was designed as a survey experiment. Gustafsson and Holmberg (2023) explain a survey experiment as a survey where respondents are given different sorts of information, stimuli, or manipulations, and then are requested to respond to given questions or statements about their experiences or opinions. This allows the researcher to assess if, or how, the stimulus affects the respondents' responses.

Furthermore, the study was designed with a mixture of a *between-subject design* and a *within-subject design*. In a between-subject design, respondents are separated into different groups and exposed to either the control condition *or* an experimental condition. In comparison, in a within-subject design, all respondents are exposed to the control condition *and* the experimental condition(s) (Gustafsson and Holmberg, 2023). In this study, all respondents' attitudes toward the organization were measured pre (being the control condition) and post one of the three experimental conditions, thus, resembling a within-subject design. However, for the study to adhere to a true within-subject design, the respondent should have been exposed to all of the study's experimental conditions (Gustafsson and Holmberg, 2023). To examine organizational reputation, a between-subject design was employed. What should be noted is that

the variable for organization reputation does not hold a control condition. This, due to the item scale used to operationalize organizational reputation (see *4.5 Key measurements*) could not be assessed by the respondents before the stimulus was presented in the survey.

4.4.2 Stimuli

The stimuli for the experimental conditions were constructed following SCCT's framework for response strategies (Coombs, 2015). Three different stimuli were constructed. Stimuli ResponseA contained the denial response strategies *scapegoat* and *victimage*, stimuli ResponseB held the diminish strategy *excuse*, and stimuli ResponseC the rebuild strategies *apology*, *ingratiation,* and *compensation*.

Stimuli	**Response strategies**
ResponseA	Deny • Scapegoat • Victimage
ResponseB	Diminish • Excuse
ResponseC	Rebuild • Apology • Ingratiation • Compensation

Figure 5. Stimuli.

A pre-test of the stimuli was conducted to ensure that the stimuli were aligned with the response strategies we aimed to assess. Wrench et al. (2013) declare that conducting a pre-test of the stimuli enhances the study's validity. Three non-related individuals, representing three different age groups, were provided with a table of SCCT's response strategies and the formulated textual responses (the stimuli). They were asked to review the responses and point out which response strategy(ies) they considered to be represented in the text. Informed by their assessments of the pre-test, two responses were slightly adjusted to improve clarity for the final stimuli (See *Attachment 9.2*).

The crisis scenario portrayed in the experiment, along with the organization and the responses, were fictional. We crafted a fictitious scenario to create a more controlled

environment for conducting the experiment, thus minimizing the risk of preconceptions or external factors that could influence participants' attitudes. At the end of the survey, respondents were informed that the scenario was fictitious, ensuring adherence to research ethics (Etikprövningsmyndigheten, 2022).

4.4.3 Questionnaire

The digital survey experiment was designed in GoogleForms. A total of three questionnaires were constructed, one for each experimental condition. The questionnaire contained 22 questions divided into five sections by themes (See *Attachment 9.1*). All questions were constructed as closed questions with default answer options, meaning the respondent could not provide individual or unique answers. Additionally, all questions were made mandatory to answer in the questionnaires for the respondent to proceed to the next section.

In the introductory section, the respondents were provided with contact details for the researchers, briefed about the aim of the study, and informed about the intended use of the collected data. Further, they were informed that participation was voluntary and anonymous (Trost & Hultåker, 2016). Ensuring anonymity can act as a motivational factor for the respondent's willingness to participate in the study (Ejlertsson, 2019).

The second section contained questions about demographics such as gender, age, and whether their place of residence was Sweden. This latter question, was a screening question, meaning if the respondent checked the box "No", the survey was automatically handed in with a greeting thanking the respondent for ze's participation.

In the third section, the respondent had to answer "Do you know what a cyber attack is?". This question was also a screening question computed as described above when the option "No" was selected. Continuing the respondent was asked to assess ze's knowledge about cyber attacks. Screening questions were included so that the respondents were solely permitted to proceed to the next question if their answers kept them within the target group for the study.

Background information about an organization subjected to cyber attacks was provided in the fourth section. Based on the information, the respondent was requested to state their level of agreement for a total of nine items measuring crisis responsibility and attitude toward the organization (see *4.5 Key measurements)*.

In the fifth section, a statement by the organization was provided, being one of the three manipulated stimuli representing the experimental conditions. Respondents were asked to read the statement in detail before proceeding to rate their level of agreement with eight items measuring organizational reputation and attitude toward the organization.

The survey questionnaires were administered via a program to make sure the three versions of the questionnaire were equally distributed. However, if a respondent clicked the link without completing the survey, the program still accounted for that as one case selection resulting in a minor difference in responses. In total, the received responses were stimuli ResponseA (44), stimuli ResponseB (37), and stimuli ResponseC (40).

A pre-test of the questionnaire was performed to detect any weaknesses or ambiguous information. The purpose of the pilot testing was to ensure the instructions and questions in the survey were properly perceived and comprehended by the participants (Wrench, Richmond & McCroskey, 2013). We received feedback regarding the items measuring attitude toward the organization. In conversation with our supervisor, the items were revised ensuring a more clear and comprehensible formulation.

4.5 Key measurements

To answer the thesis research questions, abstract concepts needed to be defined and converted into measurable variables. This process is referred to as the operationalization (Gustafsson & Holmberg, 2023). In this study, we aim to examine attitudes. Gustafsson and Holmberg (2023) suggest that attitudes can be effectively assessed in a questionnaire by presenting statements and allowing respondents to indicate their level of agreement or disagreement using a Likert scale. Pre-established scales were adapted to suit the study. Using pre-established measurement scales offers several advantages, including higher validity and reliability. Further, it ensures alignment with the theoretical framework and enables comparison of the study's results with others (Gustafsson & Holmberg, 2023). Attitudes toward an organization complement organizational reputation in an understanding of public perception (see *2. Previous research*). Based on this, two dependent variables for attitudes toward an organization and one for organizational reputation were decided to be included in the study. Considering organizational reputation as a long-term assessment (Coombs, 2015), we considered including a variable to measure instantaneous public attitudes was beneficial.

4.5.1 Dependent variables

Attitude toward the organization was measured by a three-item scale used by Lafferty and Goldsmith (2005) inspired by Spears and Singh's (2004) five-item scale which had a Cronbach's alpha of 0.97. Respondents were asked to indicate their attitudes on each of the three 7-point adjective pairs that best reflected their attitudes toward the brand. The items were ''bad/good'' "negative/positive" and "unfriendly/friendly''. The anchors were (1) bad to (7) good etc. Attitude toward the organization was measured twice, both pre and post stimuli.

Organizational reputation was measured using five items from Coombs and Holladay's (1996) ten-item Organizational Reputation Scale adapted to Swedish. The five items used in the present study were: (a) "I believe that the organization cares about its customers.," (b) "I consider the organization as dishonest.," (c) "I do not trust the organization to tell the truth about the event," (d) "I believe that what the organization says is true," and (e) "I believe that the organization does not care about the well-being of its customers." In previous research the 10-item version of the scale had a Cronbach's alpha of .82 (Coombs & Holladay, 1996) and .92 (Coombs, 1998). The anchors for the Organizational Reputation scale in this study were 1 (disagree completely) to 5 (agree completely).

4.5.2 Independent variables

Knowledge was measured using two items. One was a screening question asking the respondent whether ze knew what a cyber attack is with a simple Yes/No answer. The other item was inspired by Raju et al's (1995) scale to measure subjective knowledge. Their five-point Likert scale measured subjective or self-perceived knowledge, e.i how much consumers think they know about a product category. In this study, we similarly asked the respondents to assess their knowledge about cyber attacks. The item had anchors of 1 (no knowledge) to 5 (very good knowledge).

Crisis Responsibility was measured with a six-item scale based on Brown and Ki's (2013) twelve-item scale 'Crisis Responsibility Scale' which had a Cronbach's alpha of 0.95. They developed the scale to provide a reliable and valid measure of organizational crisis responsibility that could be uniquely applied to empirical research in crisis communications and public relations using Coombs's SCCT theory or others. It was based on Griffin, Babin, and Darden's (1992) scale for Blame and Coombs (2002) adapted item of personal control by McAuley et al.,

(1992) named Causal Dimension Scale II (CDSII) which Coombs used throughout his experimental research studies resulting in the SCCT. Furthermore, the design of our experimental study did not support 6 out of the twelve-item scale. Six items were excluded from the original scale in our study since we evaluated them as risks to confuse the respondents in regard to our scenario. Additionally, due to linguistic differences and meanings of words, we had to modify some of the items since the questionnaire was conducted in Swedish. The six items used in the study were (a) "The organization could have prevented the crisis from occurring." (b) "The organization could have prevented the consequences of the cyber attack, that sensitive information was leaked." (c) "The organization could have avoided the crisis." (d) "The organization should be held responsible for the crisis." (e) "The organization should be blamed for the crisis." (f) "The crisis was caused by a weakness in the organization". The anchors for the Crisis Responsibility scale were 1 (disagree completely) to 5 (agree completely).

4.5.3 Control variables

The study's control variables were age and gender. Age was measured with a category scale for the age group. The groups were 18-29, 30-39, 40-49, 50-59, and 60-69 years old. Gender was measured on a nominal scale with the options male, female, or other.

4.6 Analysis of data

To analyze the data IBM SPSS Statistics Version 29 was used. Firstly, the data were cleaned and preprocessed to ensure organization and accuracy. This step included recoding all answer options to numeric values, handling missing data, identifying and dealing with outliers, and ensuring data consistency (Pallant, 2020). Descriptive statistics for control and key variables were conducted to ensure normality and provide a good overview of the data. The study had a total sample of 121 respondents. One respondent was rejected in a screening question (see *4.4.3 Questionnaire*) additionally, five cases of extreme outliers were identified, leaving us with a total of 115 valid cases.

Secondly, we aimed to construct sum indexes for both dependent and independent variables (see *4.5 Key measurements*) to simplify the analysis process (Djurfeldt et al., 2018). All variables included in an index variable were coded in the same direction and assessed for internal consistency. Cronbach's alpha is a measurement for the internal consistency or reliability of a set

of items indicating the extent to which the items in the scale are correlated with each other. For the measurement to be considered valid, a score of Cronbach's alpha >0,7 or higher needs to be achieved (Pallant, 2020). We proceeded to construct index variables for dependent and independent variables as they superseded the >0,7 mark (see *Figure 6* for items included in the index variables and read more in *5.2 Internal reliability*). Additionally, descriptive statistics for index variables were conducted.

Index variable	**Included variables**
Dependent	
Index Attitudes toward Organization Pre (AOPr)	A1-A3
Index Attitudes toward Organization Post (AOPo)	A1-A3 (2)
Index Organizational Reputation (OR)	O1-O5
Independent	
Index Crisis Responsibility (CR)	C1-C6

Figure 6. Index variables.

Thirdly, one-way between-groups ANOVA with post-hoc test was performed to analyze the stimuli's (ResponseA, B, and C) effect on the dependent variables. The analysis is suitable for studies that aim to examine if there are any statistically significant differences in the means across different treatment groups (Pallant, 2020).

Lastly, two multiple regression analyses were performed with the independent variables and the experimental groups as predictors for the dependents. Multiple regression analysis is based on correlations and allows one to examine how changes in one or several independent variables are associated with changes in the dependent variable and if the changes are statistically significant (Pallant, 2020).

To enable the inclusion of the experimental conditions in the regression analysis were dummy variables for the categorical variable of the stimuli constructed. Stimulus ResponseA (*scapegoat* and *victimage*) was used as a reference category. The reference category shall be decided based on what the study aims to examine and previous research theory (IBM SPSS, n.d). Informed by previous research and SCCT, we aimed to examine whether the response strategies *excuse* (ResponseA)*, apology*, *ingratiation,* and *compensation* (ResponseC) resulted in a more positive attitude toward the organization and a stronger reputation compared to the response

strategies *scapegoat* and *victimage* (ResponseA). Thus ResponseA was designated as the reference category. Each category, except the reference one, were represented in the analysis by a binary variable (1 for present, 0 for absent) (Djurfeld et al., 2018).

4.7 Discussion of method

Djurefeldt et al. (2018) explain that research does not become scientific just because a research method is utilized. What characterizes good research is the usage of scientific theory and theoretical concepts. Likewise, quantitative research is not scientifically true solely because it is based on statistics (Djurefeldt et al., 2018). To avoid unreflected empiricism the study was based on SCCT and previous research.

A quantitative survey experiment method was chosen based on several theoretical factors. Firstly, an organization's reputation only holds value when quantified as it represents the public's assessment of the organization (Fombrun, 2012). Secondly, SCCT, the study's theoretical framework, was conducted through experiments (Coombs, 2015; Frandsen & Johansen, 2017). Thirdly, since we aimed to examine the effectiveness of response strategies, we argue that conducting a survey experiment with stimuli representing the strategies was suitable to enable a comparison (Gustafsson & Holmberg, 2023).

Criticism toward an experimental design within social science research primarily argues that it is ethically questionable, inappropriate, or unrealistic. Gustafsson and Holmberg (2023) declare that from an ethical point of view, interviews or other observations can be as problematic. It depends on how the experiment is conducted, the research design in itself is not problematic when conducted in a correct manner in regards to research ethics. Followers of the arguments that would be inappropriate, usually claim that studying causal relationships in the social sciences is not meaningful. That statement is rather a matter of personal preference. Lastly, arguments for that experiments in social science are unrealistic which affects their external validity since they often are artificial and thus not representative of the real world. The aim of experimental research is not to provide an exact representation of the real world but rather to identify causal relationships (Gustafsson & Holmberg, 2023).

An identified weakness in the study is its rather complicated data collection setup for the experimental conditions, being a mixture of a between-group and within-group design. For this study, we prioritized adopting the pre-established scales used in the construction of SCCT to

enable comparability with existing literature and to capitalize on validated measures over a rigorous data collection and sampling method. This since, due to limited resources, those aspects were considered hard to accomplish.

Further, the data collection method was a digital survey generating respondents' self-reported data. Studies based on self-reported questionnaires are reliant on the participants responding honestly (Trost & Hultåker, 2016). Additionally, Gustafsson and Holmberg (2023) list self-reported attitudes items as the least objective measurement for data. As researchers we could not oversee the participant's answers thus, the potential for a greater amount of inadmissible results exists. Furthermore, the digital distribution of the survey results in an inability to measure the study's total residual. Possibly resulting in a source of error we were unable to control which could have affected the validity (Djurfeldt et al., 2018). Further, a convenience sampling method along with a small sample size results in an inability to generalize the study's results as it is not representative of the population (Bryman & Bell, 2017).

An additional factor to consider is the usage of index variables to provide simplified measures. By combining items in an index variable one can explore multiple variables simultaneously however combining multiple variables into an index comes with the risk of oversimplifying complex phenomena and potentially compromising the validity of the measurement (Pallant, 2020).

4.8 The study's applicability

Research on managing cyber attack crises can yield important insights into how organizations should strategically shape their crisis communication, identifying both effective and ineffective strategies. This study contributes to the research field of strategic communication and crisis management by building upon existing knowledge and theory. The study's relevance increases since it is grounded in previous research and challenges, due to an identified knowledge gap, the well-established SCCT comprehensive framework (Boyle & Schmierbach, 2015).

However, solely because something is statistically proven does not mean it is practically useful or relevant (Djurefel et al., 2018) One can argue that the findings in this study may not be realistic for an organization to base decisions on during a cyber attack crisis, since other aspects, such as financial costs and resources for managing the crisis, need to be taken into account in the real world.

To maintain the quality we have consistently been conscious of the aspects concerning the validity and reliability. Internal validity refers to the legitimacy of whether the study measures what it aims to do whereas external validity refers to what degree the results as generalizable (Gustafsson & Holmberg, 2023). As mentioned several times throughout the thesis, our result can not be generalized due to a convenience sample and a limited sample size. Further, we acknowledge the challenge to our study posed by the demand for external validity, as it limits our control of the variables we have selected, disregarding countless other factors that may reflect the actual phenomenon of the public's attitudes and the organization's reputation in a cyber attack crisis.

Reliability refers to the study's replicability (Bryman & Bell, 2017). By using established scales we aimed to enhance the reliability of the study's results. Moreover, we can leverage the reliability established by the established scales which provides the study with credibility. Further, using the same measurements through studies enables compatibility with existing research.

The differences in correlation and causality are worth noting when applying a quantitative research method. Correlation describes the degree of association between two variables, causality goes a step further by establishing a direct cause-and-effect relationship between them (Djurefeldt et al., 2018). The strength of experiments lies in their ability to study causal relationships and causality. However, experiments need to be repeated and scaled to determine such relationships (Gustafsson & Holmberg, 2023).

5. Result and analysis

In the following chapter, the study's results and analysis are presented. First, is descriptive statistics provided for the study's variables to provide an overview of the data. Followed by One-way between-groups ANOVA to examine the stimuli's effect on the dependent variables. Two Multiple regression analyses were conducted to analyze the study's theoretical model and test the hypotheses formulated to research the study's aim and answer the research questions. In the last section of the chapter, the results of the hypotheses are presented.

5.1 Descriptive analysis

5.1.1 Gender

Descriptive analyses were conducted for the control variables to gain deeper insight into the demographic distribution of the survey's respondents. The study consisted of 121 participants with 115 valid observations to be included in the analysis. An observation of an overrepresentation in women (81 pcs) compared to men (34 pcs) was identified. Women accounted for 70.4% while men comprised only 29.6% of the sample population. A skewed gender distribution in voluntary survey studies is commonly observed and can be explained by the general tendency for women to exhibit a higher response rate than men (Trost & Hultåker, 2016). See *Figure 7* for a visualization of the spread of this control variable.

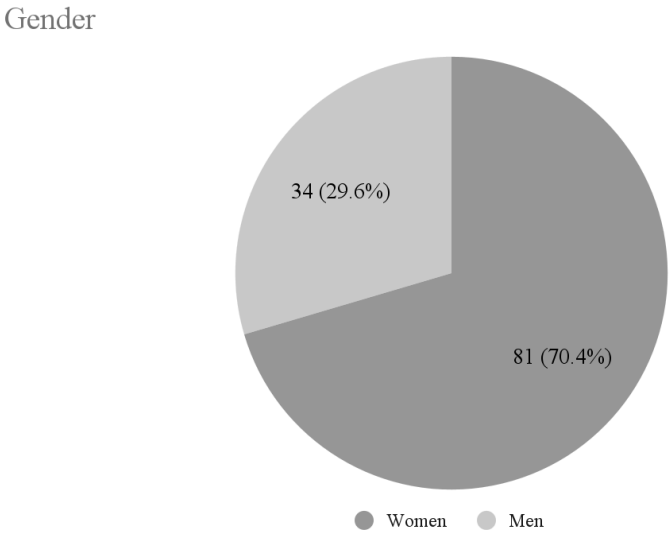

Figure 7. Distribution for gender.

5.1.2 Age

The study's respondents were categorized into five age groups 18-29, 30-39, 40-49, 50-59, and 60-69 years old. A skewed distribution, especially for the age groups 40-49 and 60-69 years was identified (see *Figure 8*). This, along with the limited sample size, affects the validity of the study's result, making it non-applicable for generalization. In *Figure 9*, the distribution of respondents' age groups are visualized.

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-29	39	33,9	33,9	33,9
	30-39	14	12,2	12,2	46,1
	40-49	7	6,1	6,1	52,2
	50-59	43	37,4	37,4	89,6
	60-69	12	10,4	10,4	100,0
	Total	115	100,0	100,0	

Figure 8. Frequencies age.

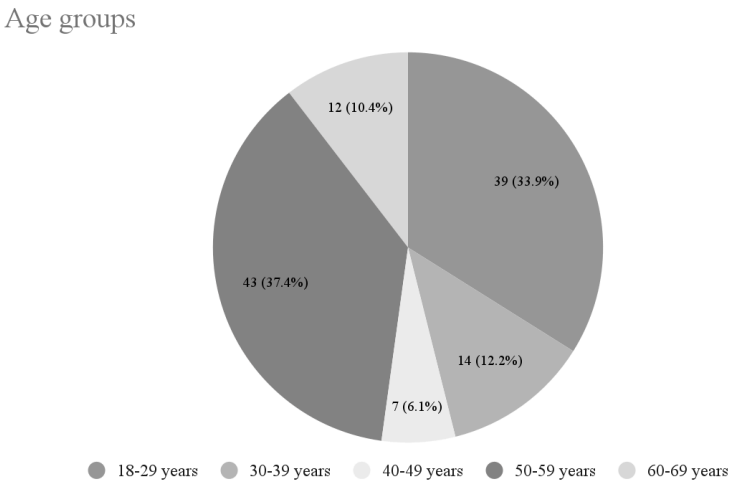

Figure 9. Distribution in age groups.

5.1.3 Stimuli

As detailed in section *4.4.3 Questionnaire*, the survey questionnaires were administered using a program to ensure equal distribution of the three versions. After excluding invalid responses and extreme outliers the number of respondents for each stimulus were ResponseA 42pcs, ResponseB 34pcs, and ResponseC 39pcs (see visualization in *Figure 10).*

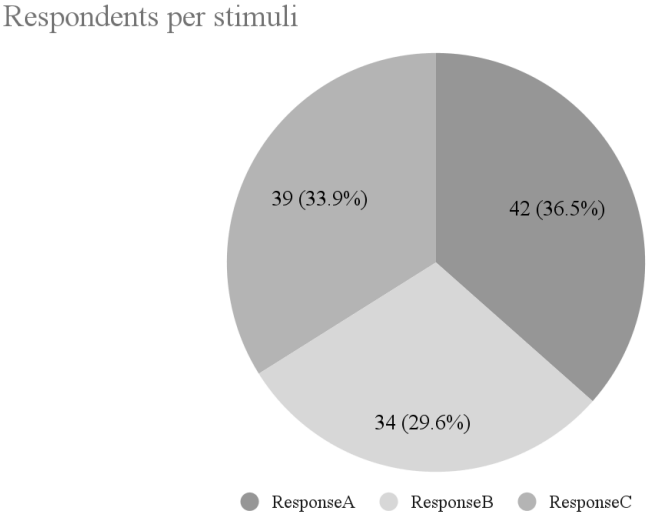

Figure 10. Distribution of stimuli.

5.1.4 Attitudes toward the Organization

To examine the impact of the different stimuli, the response strategies, on the public's attitudes toward the organization, a comparison in mean values between the experimental groups in the study was performed. Attitudes toward the Organization were measured on a 7-point Likert scale ranging from (1) bad to (7) good. The mean for ResponseA was 3,7619, ResponseB 4,1569, and ResponseC had a mean of 4,2735 (see visualization in *Figure 11*). The findings suggest that respondents exposed to ResponseA (*scapegoat* and *victimage*) had a slightly more negative attitude toward the organization compared to those exposed to ResponseB (*excuse*) and ResponseC (*apology*, *ingratiation*, and *compensation*) which further improved the attitude.

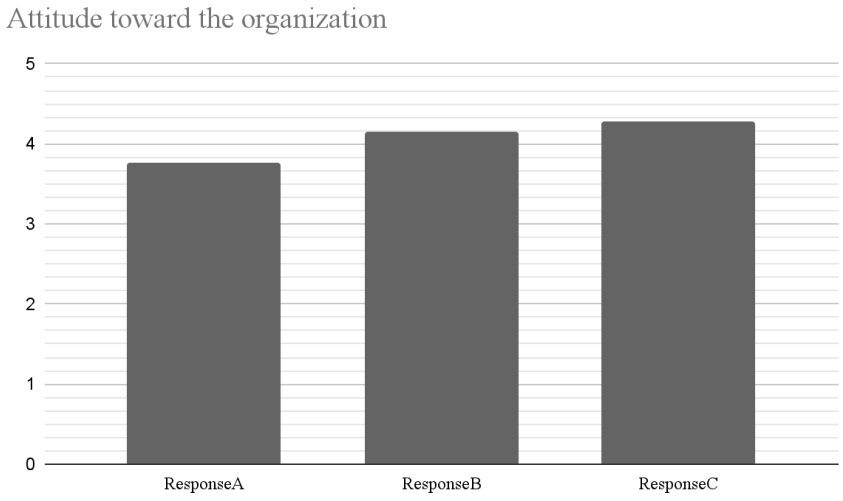

Figure 11. Stimuli effect on the public's attitudes towards the organization.

5.1.5 Organizational Reputation

To examine the impact of the different response strategies effect on the organizational reputation a comparison in mean values between the experimental groups in the study was performed. The respondents stated their level of agreement on a 5-point Likert scale where (1) indicated a weak reputation and (5) a strong reputation. ResponseA resulted in a mean value of 3,1524, ResponseB had a mean value of 3,6000, and ResponseC had a mean value of 3,7846 (see *Figure 12*). The differences in the mean values for organizational reputation indicate a variation between

the experimental groups, with the most prominent difference found in ResponseA compared to stimuli ResponseC.

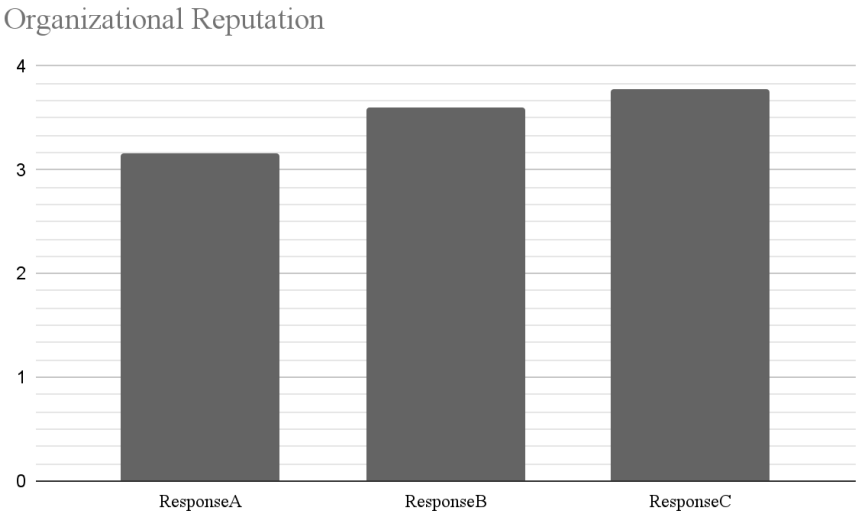

Figure 12. Bar chart for organizational reputation based on the experimental conditions.

5.1.6 Knowledge and Crisis Responsibility

The dependent variables represent the outcomes of what the study aims to measure in relation to the independent variables (Djurfeldt et al., 2018). The independent variable Knowledge (K) was measured on a 5-point Likert scale where the respondent was asked to assess ze's knowledge about cyber attacks. (1) referred to "no knowledge" and (5) referred to "very good knowledge". Crisis responsibility (CR) was also measured on a 5-point Likert scale where (1) referred to "no/minimal" crisis responsibility and (5) referred to "high" crisis responsibility. To provide an overview of the key measurements in the study, descriptive statistics of the variables' mean values and standard deviations are presented in *Figure 13* The dependent variable Attitudes toward the Organization was measured pre (AOPr) and post (AOPo) stimuli and thus is two values of it provided.

Variable	Minimum	Maximum	Mean	Std. Deviation
Dependent variables				
Attitude toward Organization Pre (AOPr)	1	6	3,8667	0,7657
Attitude toward Organization Post (AOPo)	1	7	4,0522	1,0482
Organizational Reputation (OR)	1,60	5	3,4991	0,7829
Independent variables				
Knowledge (K)	1	5	2,960	0,810
Crisis Responsibility (CR)	1,83	5	3,3899	0,6294

Figure 13. Descriptives for variables showing mean values and standard deviations.

5.2 Internal Reliability

As mentioned in *4.6 Analysis of data*, index variables were constructed for both of the dependent variables Attitudes toward the Organization and Organizational Reputation, and for the independent variable attribution of Crisis Responsibility. By combining variables into indexes, random variations are reduced and we can average out measurement noise resulting in a more reliable and stable measure of the underlying construct (Djurfeldt et al, 2018). Cronbach's alpha measures the internal consistency or reliability of a set of items indicating the extent to which the items in the scale are correlated with each other. For the measurement to be considered valid, a score of Cronbach's alpha >0,7 or higher needs to be achieved (Pallant, 2020)

The study's first dependent index variable, Attitudes toward the Organization exists in two versions, pre (AOPr) and post (AOPo) stimuli. The index variable AOPr can be interpreted as the study's control condition, allowing the assessment of changes in respondents' attitudes pre and post between the stimuli (Pallant, 2020; Gustafsson & Holmberg, 2023). The index Attitudes toward the Organization pre stimuli (AOPr), was constructed from three items in the questionnaire (A1-A3), each presented as a pair of adjectives on a 7-point Likert scale ranging from, for example, (1) "bad" to (7) "good". AOPr and achieved a Cronbach's alpha of 0,813. The same three items were used to measure the attitudes post stimuli (AOPo) and achieved r= 0,910. Thus, we could ensure that the variables were approved to create indexes from and proceed with the construction.

The second dependent variable aimed to measure Organizational Reputation. It was based on five items in the questionnaire (O1-O5) with answer options represented on a 5-point Likert scale. The respondent stated their level of agreement for five statements where (1) referred to

"disagree completely" and (5) referred to "agree completely". The less the respondent agreed with the statements the weaker organizational reputation. The items for the index Organizational Reputation questionnaire items achieved a Cronbach's Alpha of 0,858 and therefore were an index variable for Organizational Reputation (OR) constructed.

The independent variable Crisis Responsibility was measured in six items in the questionnaire (C1-C6). The items were based on the same 5-point Likert scale as Organizational Reputation. Cronbach's alpha resulted in 0,725 and an index variable was constructed.

Constructions	**Cronbach's Alpha**
Dependent	
Index Attitude toward Organization Pre (AOPr)	0,813
Index Attitude toward Organization Post (AOPo)	0,910
Index Organizational Reputation (OR)	0,858
Independent	
Index Crisis Responsibility (CR)	0,725

Figure 14. Cronbach's alpha index variables.

5.3 One-way between-groups ANOVA

5.3.1 Attitudes toward the Organization based on stimuli

A one-way between-groups ANOVA test was conducted to further examine the stimuli's impact on the dependent index variable AOPo across the groups. Levene's test for homogeneity of variance showed no violation of the assumption of homogeneity, therefore no further action was taken (Pallant, 2023).

For a finding to be considered statistically significant, the significance level needs to be <0.05 (Djurefeldt et al, 2018). In *Figure 15,* the result of the ANOVA test is displayed. Despite observing differences in the means for AOPo across the experimental conditions, the ANOVA test yielded a significance value of p=0.070, indicating no significant difference between the groups.

The *effect size* can be calculated to gain a deeper understanding of how meaningful a relationship between variables or differences between groups is. The effect size is classified as

small if 0.01-0.059, medium if 0.06-0.139, and large when >0.014 (Pallant, 2020). The effect size is calculated as *Eta squared = Sum of squares between groups/Total sum of squares* (see Figure X). For this study, the experimental conditions' effect size was considered small as the Eta square ≈0.046.

ANOVA

index_attitudePost

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	5,822	2	2,911	2,730	,070
Within Groups	119,421	112	1,066		
Total	125,243	114			

Figure 15. ANOVA index variable AOPo between stimuli.

5.3.2 Change in Attitude toward the Organization based on stimuli

As previously mentioned, the index variable Attitude toward the Organization Pre (AOPr) can be interpreted as the control condition in the study. Given the limited sample size of the study, exposing all respondents to the control condition enabled us to evaluate the normal distribution of attitudes toward the organization before any exposure to stimuli. A method to prevent the occurrence of significantly higher or lower baselines by chance before exposure to the experimental condition (Gustafsson & Holmberg, 2023).

A comparison of the change in attitude pre and post-stimuli was performed to further analyze the response strategies' effect on the public's attitudes toward the organization. The variable Change in Attitude toward the organization was calculated *AOPo - AOPr = Change in Attitude*. ResponseA had a mean value for change in attitudes of -0,0714 indicating slightly worsened attitudes post stimuli. ResponseB resulted in a mean value of +0,2353, indicating slightly improved attitudes. Finally, ResponseC had a mean of +0,4188, indicating improved attitudes (see *Figure 16*). The results indicate that the experimental condition ResponseA generated a negative attitude whereas ResponseB and ResponseC generated a more positive attitude towards the organization with the greatest effect of ResponseC.

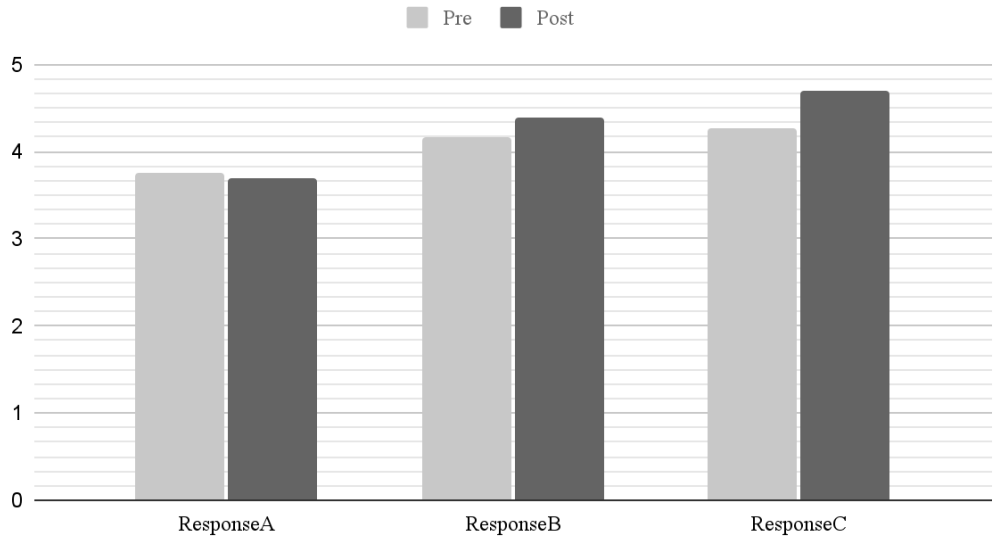

Figure 16. Mean Change in Attitude towards the Organization.

In the one-way between-groups ANOVA, statistical significance (<0,05) for the three experimental conditions' change in the attitude toward the organization was identified. Levene's test for homogeneity of variance showed no violation of the assumption of homogeneity. In *Figure 17* one can see that the statistical significance amounted to p=0.026. The effect size amounted to 0,063, indicating a medium effect (Pallant, 2020).

ANOVA

index_attitudeChange

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4,980	2	2,490	3,782	,026
Within Groups	73,730	112	,658		
Total	78,709	114			

Figure 17. ANOVA Change in Attitude.

If significance is found, Pallant (2020) suggests a further analysis of the post-hoc test provided in the Multiple Comparison table (*Figure 18*). The table allows one to see the exact differences

between the groups and in this case, the stimuli. When studying the table, a significant difference between ResponseA and ResponseC is the only one detected with p=0,021.

Multiple Comparisons

Dependent Variable: index_attitudeChange

Tukey HSD

(I) Stimuli A, B, C	(J) Stimuli A, B, C	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Response A	Response B	-,30672	,18718	,234	-,7513	,1379
	Response C	-,49023*	,18043	,021	-,9188	-,0617
Response B	Response A	,30672	,18718	,234	-,1379	,7513
	Response C	-,18351	,19037	,601	-,6357	,2687
Response C	Response A	,49023*	,18043	,021	,0617	,9188
	Response B	,18351	,19037	,601	-,2687	,6357

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

Figur 18. Post-hoc test Change in Attitude.

5.3.3 Organizational Reputation based on stimuli

To further examine the stimuli's effect, a one-way between-groups ANOVA test was also conducted for the dependent index variable Organizational Reputation and. No violation of the assumption of homogeneity was found in Levene's test for homogeneity of variance. The result p=<0,001, indicated a statistical significance of variance between the stimuli groups (see *Figure 19*.). The effect size amounted to 0,1227, indicating a large effect.

As the ANOVA showed significant variance between the experimental conditions, the analysis was followed by a Multiple Comparisons post-hoc test (Pallant, 2020). In *Figure 20*, the Multiple comparison table is provided. Informed by the table one can see that ResponseA holds a statistically significant difference between the other two experimental conditions, ResponseB (p= 0,027) and ResponseC (p=<0,001). Further, it shows that stimuli ResponseB and ResponseC do not hold significant differences between each other.

ANOVA

index_orgrep

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8,574	2	4,287	7,834	<,001
Within Groups	61,296	112	,547		
Total	69,870	114			

Figure 19. ANOVA Organizational Reputation.

Multiple Comparisons

Dependent Variable: index_orgrep

Tukey HSD

(I) Stimuli A, B, C	(J) Stimuli A, B, C	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Response A	Response B	-,44762*	,17067	,027	-,8530	-,0422
	Response C	-,63223*	,16451	<,001	-1,0230	-,2415
Response B	Response A	,44762*	,17067	,027	,0422	,8530
	Response C	-,18462	,17358	,539	-,5969	,2277
Response C	Response A	,63223*	,16451	<,001	,2415	1,0230
	Response B	,18462	,17358	,539	-,2277	,5969

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

Figure 20. Multiple comparisons table Organizational Reputation.

5.4 Multiple regression analysis

By conducting a Multiple regression analysis we aimed to test the study's full model presented in *3.2 Application of theory*. A multiple regression analysis allows an exploration of the interrelationships between several independent variables and the dependent variable (Pallant, 2020). Further, it provides statistics for how well the independent variables predict the dependent variable's outcome. For this study, the aim was to examine how knowledge about cyber attacks, attribution of crisis responsibility, and different response strategies affect the public's attitude toward the organization and the organization's reputation. Since the study's theoretical model has two dependent variables, two separate multiple regression analyses had to be performed to examine the relationships between all the variables (Pallant, 2020).

To enable the inclusion of the experimental conditions between the groups, as predictors in the regression analyses, the nominal variable indicating the stimuli were recoded into dummy variables as explained below (Djurfeldt et al, 2018).

- dummy_ResponseB: 1 for ResponseB or else 0.
- dummy_ResponseC: 1 for ResponseC or else 0.

No dummy variable was constructed for the stimuli ResponseA due to the logical reasoning that if not ResponseB nor ResponseC, it must be ResponseA. Furthermore, the experimental

condition ResponseA was left out to be used as a reference category in the multiple regression analyses. A reference category provides a baseline to which the other dummy variables are compared to (Djurfeldt et al, 2018; Pallant, 2020). ResponseA was chosen as the reference category based on the theoretical framework SCCT's claim that the response strategies *scapegoat* and *victimage*, which was the manipulation of the stimuli ResponseA, are the appropriate response strategies to utilize in a cyber attack crisis and which we aimed to explore and challenge (Coombs, 2015; Brown & Ki, 2013).

Preliminary the Multiple regression analyses were conducted, we examined whether there existed any violation of the assumption of normality, multicollinearity, and homoscedasticity in accordance with Pallant's (2020) recommendations. Additionally, we tested the model including one of the study's control variables, gender. The results displayed no significant indication for the null hypothesis "attitude is not affected by gender".

5.4.1 Multiple Regression analysis Attitudes toward the Organization

In the first regression analysis, the relationship between the independent variables' knowledge of cyber attacks (K), attribution of crisis responsibility (CR), and the stimuli were assessed as predictors for the dependent index variable Attitudes toward the organization (AOPo). The measurement R Square indicates the proportion of variation in the dependent variable explained by the independent variables (Pallant, 2020). However, when the sample size is small, R^2 tends to overestimate the true value in the population optimistically. Adjusted R Square corrects this value and provides a more accurate calculation (Djurfeld et al, 2018). The model provided a R^2=0,145 but, given our limited sample size, we opted to review the value of Adjusted R^2= 0,114 (see *Figure 21*). Thus, the predictors analyzed in the first regression analysis explains 11,4% of the variation in the dependent variable (AOPo).

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,381[a]	,145	,114	,98636

a. Predictors: (Constant), dummy_responseC, index_crisisrep, Knowledge, dummy_responseB

b. Dependent Variable: index_attitudePost

Figure 21. Model summary of Attitudes towards the Organization.

The analysis of variance (ANOVA), provides a significance test for how well the model explains the phenomenon. The limit of the significance value is 0,05 meaning a value below needs to be achieved (Pallant, 2020). Our model provided a significance of p=0,002, indicating the complete model is useful and has a high reliability.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	18,222	4	4,555	4,682	,002[b]
	Residual	107,021	110	,973		
	Total	125,243	114			

a. Dependent Variable: index_attitudePost

b. Predictors: (Constant), dummy_responseC, index_crisisrep, Knowledge, dummy_responseB

Figure 22. ANOVA Multiple regression analysis for Attitudes toward the Organization.

In the Coefficients table (*Figure 23*) the variables standardized beta coefficients (β) are presented. A positive β indicates that an increase in the predictor variable corresponds with an increase in the dependent variable, whereas a negative β means that an increase in the predictor variable corresponds to a decrease in the dependent variable (Djurfeldt et al., 2018). For this study, the variable with the most prominent effect on Attitudes toward the Organization was Crisis Responsibility (CR) β= -0,321 with a significance value of p=<,001.

Further, if one reads the table's rows for the two dummy variables, it shows that the stimuli ResponseB and C had a positive relational impact on the dependent index variable AOPo when ResponseA was used as the reference. ResponseC β=0,239 and ResponseB β=0,210. For the statistical significance, the value displayed under Sig. must be <0,05 (Pallant, 2020). Both ResponseC (p=0,018) and ResponseB (p=0,040) achieved a significance value <0,05, thus proving to be significant. Knowledge about cyber attacks (K) was the predictor with the lowest β=0,040, indicating almost no impact on Attitudes toward the Organization. Furthermore, p=0,661, proving to be insignificant.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	5,393	,576		9,359	<,001	4,251	6,535					
	Knowledge	,052	,117	,040	,439	,661	-,181	,284	-,004	,042	,039	,943	1,060
	index_crisisrep	-,535	,150	-,321	-3,567	<,001	-,832	-,238	-,298	-,322	-,314	,958	1,044
	dummy_responseB	,481	,231	,210	2,080	,040	,023	,939	,065	,195	,183	,760	1,316
	dummy_responseC	,527	,219	,239	2,401	,018	,092	,962	,152	,223	,212	,784	1,275

a. Dependent Variable: index_attitudePost

Figure 23. Coefficient table Attitudes toward the Organization

The *Normal Probability Plot* from the analysis (see *Figure 24*) displayed an acceptable alignment with the diagonal line indicating that the data is normally distributed and with no major deviations (Pallant, 2020).

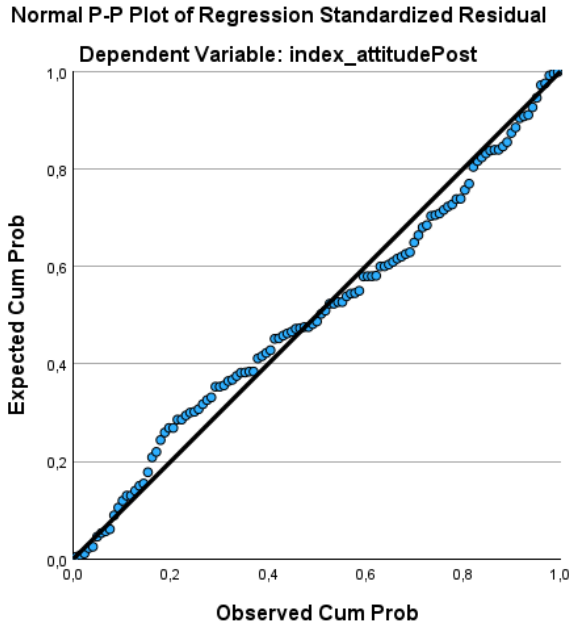

Figure 24. Normal Probability Plot from multiple regression analysis Attitude toward the Organization.

5.4.2 Multiple regression analysis Organizational Reputation

The second regression analysis examined the relationship between the dependent variable Organizational Reputation (OR) and the predictors Knowledge of cyber attacks (K), Crisis Responsibility (CR), and the experimental conditions. The analysis provided an adjusted R^2= 0,121, indicating that 12,1% of the variation in the dependent variable (OR) can be explained by the independent variables K, CR, and the stimuli (*see Figure 25)*. The ANOVA test for the model

provided a significance of 0,001, indicating the complete model is useful and has a high reliability (*Figure 26*).

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,390[a]	,152	,121	,73379

a. Predictors: (Constant), dummy_responseC, index_crisisrep, Knowledge, dummy_responseB

b. Dependent Variable: index_orgrep

Figure 25. Model summary for Organizational Reputation.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10,640	4	2,660	4,940	,001[b]
	Residual	59,230	110	,538		
	Total	69,870	114			

a. Dependent Variable: index_orgrep

b. Predictors: (Constant), dummy_responseC, index_crisisrep, Knowledge, dummy_responseB

Figure 26. ANOVA multiple regression analysis of the dependent variable Organizational Reputation.

Informed by the Coefficients table (*Figure 27*), one can see that the stimuli were the predictors with the most prominent effect on the dependent index variable Organizational Reputation (OR). With ResponseA as a reference category, the variables for the other stimuli showed a high impact on the organizational reputation. ResponseB had a β=0,264 and p=0,010 followed by ResponseC with a β=0,389 and p=<,001, proving significance. The independent variable Crisis Responsibility (CR) had a value of β= -0,153 and a significance of p=0,092 whereas Knowledge had a β=0,111 and p=0,220. Consequently, both predictor's impact proved to be statistically insignificant.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	3,473	,429		8,102	<,001	2,623	4,322					
	Knowledge	,108	,087	,111	1,233	,220	-,065	,281	,093	,117	,108	,943	1,060
	index_crisisrep	-,190	,112	-,153	-1,700	,092	-,411	,031	-,116	-,160	-,149	,958	1,044
	dummy_responseB	,452	,172	,264	2,626	,010	,111	,793	,084	,243	,231	,760	1,316
	dummy_responseC	,641	,163	,389	3,925	<,001	,317	,964	,262	,351	,345	,784	1,275

a. Dependent Variable: index_orgrep

Figure 27. Coefficient table Organizational Reputation.

The Normal Probability Plot for the second multiple regression analysis displays a strong alignment with the diagonal line indicating that the data is normally distributed and with no major deviations.

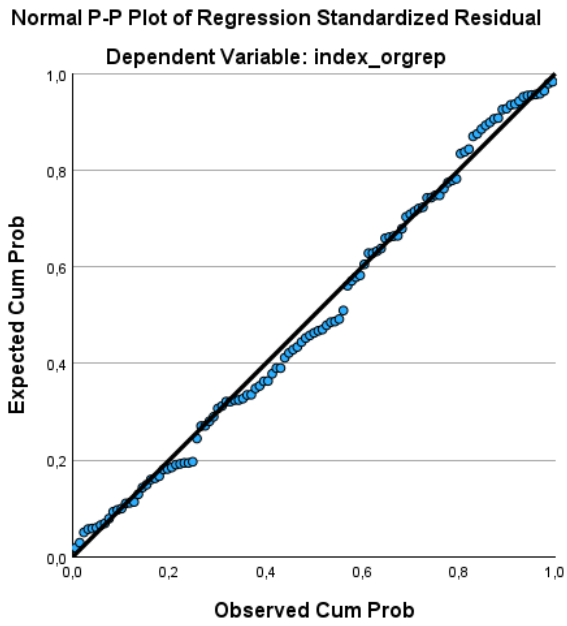

Figure 28. Normal Probability Plot from multiple regression analysis of the dependent variable Organizational Reputation.

5.4.3 Evaluation of the full model

As explained in *5.4 Multiple regression analysis*, two separate analyses were conducted since the study's model incorporated two dependent variables. Consequently, the R^2, or more accurately, the Adjusted R^2 generated by each analysis, does not fully represent the entirety of the model. To calculate the full model's R^2, the following equation can be employed: *Total* $R^2 = 1 - ((1 - R^2 1) \times (1 - R^2 2))$ (UCLA, n.d). It is important to note that a manual calculation of the total R^2 for two regression analyses should only be pursued if the dependent variables are not strongly correlated (IBM, n.d). In the Correlations table (*Figure 29*), the correlation coefficient between AOPo and OR is 0,517, falling below the 0,7 mark which is the accepted value for high correlation. This indication justified proceeding with a manual calculation of the Adjusted total R^2.

Total R^2 = 1 - ((1 - $R^2$1) x (1 - $R^2$2))

$R^2$1 = 0.114

$R^2$2 = 0.121

Total R^2 = 1 - ((1 - 0.114) x (1 - 0.121))

= 1 - (0.886 x 0.879)

= 1 - 0.778794

≈ 0.221206 = 22,12%

The resulting value of 22.12% indicates the proportion of variance in the dependent variables explained by the study's full model.

Correlations

		index_attitudePost	index_orgrep
index_attitudePost	Pearson Correlation	1	,507**
	Sig. (2-tailed)		<,001
	N	115	115
index_orgrep	Pearson Correlation	,507**	1
	Sig. (2-tailed)	<,001	
	N	115	115

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

Figure 29. Correlation between the dependent variables Attitudes towards the Organization and Organizational Reputation.

5.5 Hypotheses testing

The table below (*Figure 30*), provides an overview of the results of the multiple regression analyses including the standardized beta coefficients (β), statistical significance levels, and the decisions we have made regarding the hypotheses. A positive β signifies that as the predictor variable increases, so does the dependent variable, while a negative β suggests that an increase in the predictor variable leads to a decrease in the dependent variable (Pallant, 2020). The hypotheses were either confirmed or rejected. For a hypothesis to be considered confirmed, the purported effect of independent variables as a predictor for the dependent variable's outcome was supported by the study's empirics with statistical significance. If the hypothesis was rejected, no

statistical significance was proved (Gustafsson & Holmberg, 2023). In summary, the result of our analysis showed that seven out of the ten relationships had a p-value <0,05, indicating statistical significance, and thus were those hypotheses considered confirmed (**H2a**, **H3a, H3b, H4a, H4b, H5a**, and **H5b**). Three of the hypotheses were rejected (**H1a**, **H1b**, and **H2b**). The model's Adjusted R^2 was 22,12%.

The study's first hypothesis **H1a**, was rejected due to a low β=0,040 and a high p=0,661. The result for the independent variable K means that knowledge about cyber attacks did not contribute to a valid explanation of the dependent variable Attitudes toward the Organization's (AOPo) outcome. Likewise was, hypothesis **H1b**, Knowledge as a predictor for Organizational Reputation (OR), rejected. Analyzing the table, one can see that the independent variable K had a higher standardized beta coefficient of β= 0,111, and an improved p-value of p=0,220 for OR compared to AOPo. However, the value did not meet the required level for statistical significance, and thus, was the hypothesis rejected.

Hypothesis **H2a** was confirmed. The predictor attribution of Crisis Responsibility (CR) showed a negative correlation with the dependent variable AOPo with a β= -,321. This means that an increase of 1 in CR results in a -0,321 worsened Attitudes toward the Organization (Djurfeldt et al, 2018). The statistical significance for the relationship was p= <0,001 indicating significance. For hypothesis **H2b**, a negative relation between CR and OR with β= -,153 was detected. However, the statistical significance level was not significant since p=0,092. Thus, **H2b** was rejected.

To assess the study's remaining hypotheses related to the stimuli's effect on the Attitudes toward the Organization and the Organizational Reputation, we will first revisit the one-way between-groups ANOVA tests (Figure 15, 17, 18, 19, and 20). The One-way between-groups ANOVA showed a significance of p=0,070 between the stimuli groups for Attitudes toward the Organization indicating no significant variations. However, when analyzing the Change in Attitude, the descriptive statistics showed a negative change for ResponseA whereas B and C had positive outcomes post stimuli. Additionally, p=0,026 in the ANOVA test thus, followed up by post-hoc test which indicated significance in the change of attitude between ResponseA and C. For organizational reputation, the ANOVA showed a significance <0,001 between the groups, indicating significant variations. The post-hoc test displayed statistical significance for ResponseA compared to B (p=0,027) and C (p=<0,001) but not for ResponseB compared to C

(p=0,539). In the multiple regression analyses, ResponseA was used as a reference category. Consequently, ResponseA's standardized coefficient beta was β =0. The variable used as a reference represents a baseline of comparison and thus, has no actual change in the dependent variable (Pallant, 2020). The significance value for the experimental condition ResponseA, is shown in the coefficient tables in *Figure 23* and *27* in the row (Constant). The significance was p= <0,001 in both multiple regression analyses. Based on the presented results above, both **H3a** and **H3b** were considered confirmed. To clarify, the response strategies *victimage* and *scapegoat* generated a worsened attitudes toward the organization and resulted in the weakest organizational reputation in comparison to the other two experimental conditions.

Hypotheses **H4a** and **H4b** referred to the experimental condition ResponseB. ResponseB as a predictor for the dependent variable AOPo resulted in a β = 0,210 and a significance of p=0,040, confirming the hypothesis **H4a**. Likewise, was **H4b** confirmed with a β =0,264 and p=0,010. Further, **H5a** and **H5b**, stating the study's expected relationship between stimuli ResponseC and the dependent variables were both confirmed. **H5a** resulted in a β = 0,239 and p=0,016. **H5b** β = 0,389 was the study's predictor with the greatest impact on a dependent variable, p=<0,001.

Hypothesis	Effect	β=Beta	Sig.	Decision
H1a	K → AOPo	0,040	0,661	Rejected
H1b	K → OR	0,111	0,220	Rejected
H2a	CR → AOPo	-0,321	<0,001	Confirmed
H2b	CR → OR	-0,153	0,092	Rejected
H3a	RespA → AOPo	0	<0,001	Confirmed
H3b	RespA → OR	0	<0,001	Confirmed
H4a	RespB → AOPo	0,210	0,040	Confirmed
H4b	RespB → OR	0,264	0,010	Confirmed
H5a	RespC → AOPo	0,239	0,018	Confirmed
H5b	RespC → OR	0,389	<0,001	Confirmed

Figure 30. Hypotheses results and decision overview.

6. Discussion

In the following section, we discuss what the study's results and general discoveries mean both in a larger context but also in relation to the expected results. Further, we reflect on a secondary finding between the two dependent variables.

The emergence of the new context that the crisis type cyber attacks seem to provide coupled with the yearly increased numbers of attacks has created a need for further research. Previous research has emphasized that the public's perception of organizations subjected to a cyber attack may not align with SCCT's *victim* categorization (Krishna & Vibber, 2017). According to SCCT, a cyber attack will attribute minimal crisis responsibility toward the organization and hence have a minimal impact on organizational reputation. Thus the response strategies *scapegoat* and *victimage* should be suitable to manage the crisis (Coombs & Holladay, 1996; Coombs, 2015). Our findings suggest that the utilization of those strategies results in a negative impact on the public's attitudes toward the organization and the organizational reputation. Instead, the response strategies *excuse, apology, ingratiation,* and *compensation* were statistically found to be effective. The result contradicts what the framework of SCCT declares, being that an organization subjected to a malicious act is perceived as a victim by the public and thus, should utilize the first-mentioned strategies. Our results were in line with Kuipers and Schonheit's (2022) findings, suggesting that organizations should admit responsibility rather than employ denial and victimage strategies in a cyber attack crisis to protect their reputation.

Attribution of crisis responsibility was found to negatively affect attitudes toward the organization but not the organization's reputation in this study which contradicts SCCT (Coombs, 2015). As discussed and explained earlier in the thesis, organizational reputation is constructed from a long-term relationship including history. The fact that the organization in the experiment was fictitious could thus have affected the respondents' evaluation since no prior relationship existed. However, crisis responsibility was found to have a negative effect on

attitude toward an organization. This finding is in line with Lafferty and Goldsmith's (2005) explanation that attitudes are formed more instantaneously and based on a situation.

Our findings are even more interesting when related to the definitions of organizational reputation and attitudes. Organizational reputation encompasses the overall perception of an organization while attitudes focus on individuals' specific feelings and evaluations of that organization. Attitudes contribute to the formation and maintenance of an organization's reputation, but reputation extends beyond individual attitudes to represent the total public perception of the organization within its environment (Coombs, 2015, Lafferty and Goldsmith, 2005). This means that an individual's attitudes constitute the collective and the collective constitutes the individual. Therefore, both the public's attitudes toward the organization and the organizational reputation were examined. An interesting secondary finding in the study's result was that the two variables were not strongly correlated.

Informed by previous research about how high individual knowledge of a subject can result in skepticism, the study predicted that a knowledgeable individual in the field of cybersecurity and cyber attacks would hold a more negative attitude toward an organization subjected to an attack (Raju et al., 1995; Romani et al., 2016). This is since they were likely to hold higher expectations for an organization to withstand an attack and/or demand more detailed information about the attack. However, the study found no significant relationship between individual knowledge and attitudes toward an organization subjected to a cyber attack, neither negative nor positive. Further, high knowledge did not affect individuals' perception of the organization's reputation more negatively. It should be noted that knowledge of cyber attacks in this study was measured through self-reported and self-evaluated data. Therefore and following our post-positivist approach, we argue that the level of knowledge should continue to be researched concerning how individuals perceive organizations in crises.

The results of the study raise the question of whether a cyber attack crisis can be managed per the SCCT's framework. If not, how should the crisis type be assessed and managed to ensure the protection of an organization's reputation? Even though several hypotheses showed statistically significant results, it is important to recognize that additional factors may influence attitudes. Examining only a single crisis and utilizing one theoretical framework cannot produce generalizable knowledge. Due to the study's scope, several other potential factors were excluded even though previous research may highlight their relevance. Therefore, we encourage future

research to continue to explore a broader perspective of the phenomenon of cyber attacks as a crisis. Finally, we wish to emphasize that the scope and resources of this thesis should be considered as possible influences on the results.

7. Conclusion

In the final chapter of this thesis, we answer the study's research questions and present our conclusions. This is followed by a discussion of how the study's results can serve as a basis for future research, as well as some of its limitations.

This study aimed to contribute knowledge about the crisis type cyber attacks by analyzing a cyber attack crisis' effect on public attitudes toward organizations and the organizational reputation. The study examined if knowledge about cyber attacks, attribution of crisis responsibility, and different response strategies had an effect on the public's attitude toward an organization and the organizational reputation in the context of a cyber attack crisis. The results of the study showed that the employed response strategies along with the independent variable crisis responsibility had the greatest impact on the organization's reputation. Further, the response strategies also had the greatest impact on individuals' attitudes toward the organization.

The first research question was as follows RQ1: *Does an individual's knowledge of cyber attacks influence the attitudes toward an organization and the organization's reputation during a cyber attack crisis?* The study's hypotheses **H1a** and **H1b** were constructed to answer the research question. Our findings did not suggest that an individual's level of knowledge influences ze's attitude toward or the organizational reputation. In fact knowledge was found to be the least impactful predictor for the dependent variables.

Hypothesis **H2a** and **H2b** aimed to answer the research questions RQ2a: *How does attribution of crisis responsibility impact the attitudes toward an organization and the organization's reputation when subjected to a cyber attack?* and RQ2b: *To what extent does the public attribute crisis responsibility to an organization subjected to a cyber attack?* Crisis responsibility was statically proven to have negative effects on the public's attitudes toward an organization. Further, it had negative effects but not statistically significant on the organization's reputation. Regarding to what extent the public attributes crisis responsibility to an organization

subjected to a cyber attack the independent index variable CR's mean amounted to 3,3899 on a measurement scale (1) to (5). Based on this, the level of attribution of crisis responsibility should be understood as moderate towards high.

For research question RQ3: *What response strategies have positive effects on organizational reputation and attitudes toward an organization when an organization has been subjected to a cyber attack crisis?* The experimental condition including the response strategies *apology, ingratiation,* and *compensation* was proved with statistical significance to be the response strategies with the greatest positive effect on both the attitudes toward the organization and the organization's reputation. Furthermore, the response strategy *excuse* was also found to result in a stronger reputation and have positive effects on attitudes. The results are in line with the findings of Kuipers & Schonheit (2022), indicating denial strategies are ineffective when managing a cyber attack crisis.

The study's last research question RQ4: *Is an organization subjected to a cyber attack perceived by the public in line with the victim crisis frame of Coomb's Situational Crisis Communication Theory?* was formulated more openly to allow a greater interpretation of the study's findings. The study's model was found to explain 22,12% of the variation in the dependent variables. Based on the study's findings, we concluded that when an organization experiences a cyber attack, the public does not perceive it in line with SCCT's victim crisis frame.

7.1 Limitations and future research

Due to the study's sampling method and limited sample size, the results and conclusions can not be generalized. Future research analyzing how cyber attacks affect organizational reputation should aim for a larger representative sample and rigorous sampling methods to ensure the generalizability of the findings. However, our study's finding suggests that a cyber attack crisis may not be able to be managed through SCCT's framework. We encourage future research to continue exploring the crisis type of cyber attack crises and how to manage them.

Rejected hypotheses should be revisited (Ryan, 2006). For example, we argue that knowledge is an interesting variable to further investigate within the field of strategic communication since it could lead to a better understanding of the need for individualized communication. In this study, the respondent evaluated their knowledge about cyber attacks,

resulting in a subjective measure for the variable. Brucks (1985) differentiates objective and subjective knowledge. He defines objective knowledge as what actually is ‘stored’ in an individual's memory whereas subjective knowledge reflects what an individual perceives they know (Brucks, 1985). Therefore, to gain more reliable results, future studies should apply an approach where objective knowledge is taken into account.

Lastly, globalization and technological development have resulted in a higher demand for research exploring cultural differences in crisis management and public relations. Today, organizations and crisis managers need to take cultural differences into account when managing a crisis due to, among other things, the power of social media in connecting the world despite geographical distances (Zhao, 2021). Thus a comparison study to explore and examine differences between nations or cultures would be desirable when it comes to the public’s perception of the phenomenon of cyber attack crises’ impact on organizational reputation and could contribute to a better understanding and guide global organizations in their crisis management.

8. Reference

Allen, M. W., & Caillouet, R. H. (1994). Legitimation Endeavors: Impression Management Strategies Used by an Organization. *Communication Monographs, 61*(1), 44-62. https://doi.org/10.1080/03637759409376322

Bae, M. (2018). Overcoming skepticism toward cause-related marketing claims: The role of consumers' attributions and a temporary state of skepticism. *Journal of Consumer Marketing,* 35(2), 194–207. https://doi.org/10.1108/JCM-06-2016-1827

Boyle, M., & Schmierbach, M. (2015). *Applied Communication Research Methods: Getting Started as a Researcher* (1ed.). Routledge.

Brown, A. K., & Ki, E.-J. (2013). Developing a Valid and Reliable Measure of Organizational Crisis Responsibility. *Journalism & Mass Communication Quarterly, 90*(2), 363-384. https://doi.org/10.1177/1077699013482911

Brucks, M. (1985). The effects of product class knowledge on information search behavior. *Journal of Consumer Research, 12*(1), 1–16. https://doi.org/10.1086/209031

Bryman, A., & Bell, E. (2017). Företagsekonomiska forskningsmetoder. Stockholm: Liber.

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*(3), 256–262. 10.1016/j.pubrev.2010.05.004

Coombs, W. T. (1995). Choosing The Right Words: The Development of Guidelines for the Selection of the "Appropriate" Crisis-Response Strategies. *Management Communication Quarterly, 8*(4), 447-476. https://doi.org/10.1177/0893318995008004003

Coombs, W. T. (1998). An Analytic Framework for Crisis Situations: Better Responses From a Better Understanding of the Situation. *Journal of Public Relations Research, 10*(3), 177-191. https://doi.org/10.1207/s1532754xjprr1003_02

Coombs, W. T. (2006). The Protective Powers of Crisis Response Strategies: Managing Reputational Assets During a Crisis. J*ournal of Promotion Management,* 12(3–4), 241–260. https://doi.org/10.1300/J057v12n03_13

Coombs, W, T. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. *Corporate Reputation Review, 10* (3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Coombs, W. T. (2015). *Ongoing Crisis Communication; Planning, Managing, and Responding.* (4th ed.). Los Angeles: Sage.

Coombs, W. T., & Holladay, J. S. (1996). Communication and Attributions in a Crisis: An Experimental Study in Crisis Communication. *Journal of public relations research. 8*(4). 279-295. 10.1207/s1532754xjprr0804_04

Coombs, W. T., & Holladay, J. S. (2002). Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory. *Management communication quarterly, 16*(2), 165-186. https://doi.org/10.1177/089331802237233

Craig, R. T., & Muller, H. L. (2007). *Theorizing Communication: Reading Across Traditions.* Sage Publications.

Djurfeldt, G., Larsson, R., & Stjärnhagen, O. (2018). *Statistisk verktygslåda 1 : samhällsvetenskaplig orsaksanalys med kvantitativa metoder* (3ed). Studentlitteratur.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral Response to Phishing Risk. Friestad*Proceedings of the Anti-phishing Working Groups 2nd Annual Ecrime Researchers Summit,* 10(4), 37-44. https://doi.org/10.1145/1299015.1299019

Ejlertsson, G. (2019). *Enkäten i praktiken: en handbok i enkätmetodik* (4ed). Lund: Studentlitteratur.

Falkheimer, J. & Heide, M. (2022). Strategic Improvisation in Crisis Communication. In The Handbook of Crisis Communication (eds W.T. Coombs and S.J. Holladay). https://doi.org/10.1002/9781119678953.ch27

Fombrun, C. J. (2012). The building blocks of corporate reputation: Definitions, antecedents, consequences. In M. L. Barnett & T. G. Pollock (Eds.), *The Oxford Handbook of Corporate Reputation* (p. 94-113). Oxford University Press.

Frandsen, F., & Johansen, W. (2017). *Organizational Crisis Communication.* Sage Publications Inc.

Friestad, M., & Wright, P. (1994). The Persuasion Knowledge Model: How people cope with persuasion attempts. *Journal of Consumer Research, 21*(1), 1–31. https://doi.org/10.1086/209380

Gray, E., & Balmer, J. (1998). Managing Corporate Image and Corporate Reputation. *Long Range Planning, 31*(5), 695-702. https://doi.org/10.1016/S0024-6301(98)00074-0

Griffin, M., Babin, B. J., & Darden, W. R. (1992). Consumer Assessments of Responsibility for Product-Related Injuries: The Impact of Regulations, Warnings, and Promotional Policies. *Advances in Consumer Research,* 19, 870-878.

Gustafsson, N., & Holmberg, N. (2023). *Experiment.* Studentlitteratur AB.

IBM, (2023). *Cost of a Data Breach Report 2023*. IBM. https://www.ibm.com/reports/data-breach (Retrieved 01-04-2024)

IBM, (n.d). *What is a cyberattack?* IBM. https://www.ibm.com/topics/cyber-attack (Retrieved 20-04-2024)

Jallinoja, P., & Aro, A. R. (2000). Does Knowledge Make a Difference? The Association Between Knowledge About Genes and Attitudes Toward Gene Tests. *Journal of Health Communication, 5*(1), 29-39. 10.1089/gtmb.2012.0350

Johansen, W., & Frandsen, F. (2007) *Krisekommunikation: Når virksomhedens image og omdømme er trust.* Frederiksberg: Samfundslitteratur.

Krishna, A., & Vibber, K. S. (2017). Victims or conspirators? Understanding a hot-issue public's online reactions to a victim cluster crisis. *Journal of Communication Management, 21*(3), 303-318. 10.1108/JCOM-08-2016-0067

Kuipers, S., & Schonheit, M. (2022). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. *Corporate Reputation Review,* 25 176–197. https://doi.org/10.1057/s41299-021-00121-9

Lafferty, A. B., & Goldsmith, E. R. (2005). Cause–brand alliances: does the cause help the brand or does the brand help the cause? *Journal of Business Research, 58*(4), 423-429. https://doi.org/10.1016/j.jbusres.2003.07.001

Ma, L., & Zhan, M. (2016). Effects of attributed responsibility and response strategies on organizational reputation: A meta-analysis of situational crisis communication theory research. *Journal of Public Relations Research, 28*(2), 102-109. https://doi.org/10.1080/1062726X.2016.1166367

McAuley, E., Duncan, T. E., & Russell, D. W. (1992). Measuring causal attributions: The revised causal dimension scale (CDSII). *Personality and Social Psychology Bulletin*, *18*(5), 566-573. https://doi.org/10.1177/0146167292185006

Mikušová, M., & Horvathova, P. (2019). Prepared for a crisis? Basic elements of crisis management in an organisation. *Economic Research, 32*(1), 1844-1868. https://doi.org/10.1080/1331677X.2019.1640625

Mitroff, I. I., & Pearson, C. M. (1993). *Crisis Management: A Diagnostic Guide for Improving Your Organization`s Crisis-Preparedness.* Jossey-Bass Publishers.

Myndigheten för samhällskydd och beredskap. (2024) Nationellt center för cybersäkerhet (NCSC). 9 feb 2024. MSB.se https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samhallets-arbete-for-okad-cybersakerhet/nationellt-center-for-cybersakerhet-ncsc/

Pallant, J. (2020). *SPSS survival manual : a step by step guide to data analysis using IBM SPSS* (7th edition). Open University Press, McGraw-Hill.

Paraskevas, A. (2006). Crisis Management or Crisis Response System? A Complexity Science Approach to Organizational Crises. *Management Decision, 44*(7), 892-907. https://doi.org/10.1108/00251740610680587

Raju, P. S., Lonial, S. C., & Mangold, W. G. (1995). Differential Effects of Subjective Knowledge, Objective Knowledge, and Usage Experience on Decision Making: An Exploratory Investigation. *Journal of Consumer Psychology, 4*(2), 153–180. http://www.jstor.org/stable/1480516

Romani, S., Grappi, S., & Bagozzi, R. P., (2016). Corporate Socially Responsible Initiatives and Their Effects on Consumption of Green Products. *Journal of Business Ethics, 135*(2), 253-264. 10.1007/s10551-014-2485-0

Rosenbaum-Elliot, R., Percy, L., & Pervan, S. (2015). *Strategic Brand Management* (3ed). Oxford University Press.

Roškot, M., Wanasika, I., & Kreckova Kroupova Z. (2021). Cybercrime in Europe: surprising results of an expensive lapse. *Journal of Business Strategy, 42*(2), 91-98. https://doi.org/10.1108/JBS-12-2019-0235

Rousseau, M. D. (2006). Is there Such a thing as "Evidence-Based Management"? *Academy of Management Review. 31*(2), 256-269. https://doi.org/10.5465/amr.2006.20208679

Ryan, B. A. (2006) P*ost-Positivist Approaches to Research. In: Researching and Writing your thesis: a guide for postgraduate students*. MACE: Maynooth Adult and Community Education, 12-26.

Sahin, S., Ulubeyli, S., & Kazaza, A. (2015). Innovative Crisis Management in Construction: Approaches and the Process. *Procedia – Social and Behavioral Sciences, 195*, 2298-2305. 10.1016/j.sbspro.2015.06.181

Spears, N., & Singh, N. S. (2004). Measuring Attitude toward the Brand and Purchase Intentions. *Journal of Current Issues and Research in Advertising, 26*(2). 53-66 https://www.tandfonline.com/doi/abs/10.1080/10641734.2004.10505164

Trost, J., & Hultåker, O. (2016). *Enkätboken* (5ed). Lund: Studentlitteratur AB.

UCLA. (n.d). *REGRESSION ANALYSIS | SPSS ANNOTATED OUTPUT.* UCLA. https://stats.oarc.ucla.edu/spss/output/regression-analysis/ (Retrieved 15-05-2024)

Verhoeven, J. W. M., Van Hoof, J. J., Ter Keurs, H., & Van Vuuren, M. (2012). Effects of apologies and crisis responsibility on corporate and spokesperson reputation. *Public Relations Review, 38*(3), 501–504. 10.1016/j.pubrev.2012.02.002

Wahab, F., Khan, I., Kamontip, Hussain, T., & Amir, A., (2023) An investigation of cyber attack impact on consumers' intention to purchase online, *Decision Analytics Journal, 8*, 1-9. https://doi.org/10.1016/j.dajour.2023.100297

Wang, P., & Johnson, C. (2018). CYBERSECURITY INCIDENT HANDLING: A CASE STUDY OF THE EQUIFAX DATA BREACH. *Issues in Information Systems. 19*(3), 150-159. https://doi.org/10.48009/3_iis_2018_150-159

Wang, P., & Park, S. (2017). COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING. *Issues in Information Systems. 18*(2), 136-147. https://doi.org/10.48009/2_iis_2017_136-147

Weick, K. E., (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies, 25*(4), 305-317. https://doi.org/10.1111/j.1467-6486.1988.tb00039.x

Weiner, B., Graham, S., & Chandler, C. (1982). Pity, anger, and guilt: An attributional analysis. *Personality and Social Psychology Bulletin, 8*(2), 226-232. https://doi.org/10.1177/0146167282082007

Wrench, J. S., Thomas-Maddox, C., Richmond, V. P., & McCroskey, J. C. (2013). *Quantitative research methods for communication: a hands-on approach.* New York: Oxford University Press.

Zerfass, A., & Verčič, D., Nothhaft, H., & Werder, K. P. (2018). Strategic Communication: Defining the Field and its Contribution to Research and Practice. International Journal of Strategic Communication, 12(4), 487-505 doi.10.1080/1553118X.2018.1493485

Zerfass, A., & Viertmann, C. (2017). Creating business value through corporate communication: A theory-based framework and its practical application. *Journal of Communication Management, 21*(1), 68-81. 10.1108/JCOM-07-2016-0059

Zhao, H. (2021). Beyond culture: Advancing the understanding of political and technological contexts in crisis communication. *International Communication Gazette,* 83(5), 517-537. https://doi.org/10.1177/17480485211029066

9. Attachments

9.1 Survey

Organisationers kommunikation vid kris

Tack för att du tar dig tid att svara på vår enkät!

Vi är två studenter från Lunds universitet som skriver vår kandidatuppsats i strategisk kommunikation inom ämnesområdet kriskommunikation. Vi ämnar undersöka hur sättet organisationer kommunicerar vid kris påverkar konsumenters attityd till dem.

Enkäten tar ca 10 minuter att svara på. Svaren är anonyma och endast ämnade att använda i statistiskt syfte till ovan beskriven studie. Observera att din medverkan sker frivilligt.

Enkäten riktar sig till dig som är 18-69 år och bosatt i Sverige.

Om du har några frågor eller funderingar kring undersökningen, kontakta
Ella Ryan: el7484ry-s@student.lu.se
Märta Söderberg: ma7423so-s@student.lu.se

Vilket kön identifierar Du dig med? *

- [ ] Kvinna
- [ ] Man
- [ ] Annat

Hur gammal är Du? *

- ◯ Under 18 år.
- ◯ 18-29 år
- ◯ 30-39 år
- ◯ 40-49 år
- ◯ 50-59 år
- ◯ 60-69 år

Bor Du i Sverige? *

- ◯ Ja
- ◯ Nej

Vet du vad en cyberattack är? *

- ◯ Ja
- ◯ Nej

Bedöm din kunskap om cyberattacker. (1) ingen kunskap, (2) begränsad kunskap, (3) måttlig kunskap, (4) god kunskap, (5) mycket god kunskap. *

	1	2	3	4	5	
ingen kunskap	◯	◯	◯	◯	◯	mycket god kunskap

Krisen. Nedan finns en beskrivning av en krishändelse. Efter att du har läst texten kommer du få svara på ett antal påståenden om dina åsikter om företaget. Svara utifrån vad dina instinktiva åsikter är.

Omfattande cyberattack mot företaget Kartula AB.

Under gårdagen drabbades Kartula av en omfattande cyberattack. Stora mängder data har läckt, både känslig information om företagets kunder och om företagets verksamhet.

Vid 8-tiden på morgonen upptäckte företaget problem med sin hemsida. Strax därefter eskalerade attacken till en massiv spammailskampanj mot medarbetarna. Företaget Kartulas it-system kunde inte stå emot attacken.

Attacken resulterade i att känslig data läckte ut vilken nu sprids på nätet. Informationen som sprids är kunders personnummer, adress, mejl, telefonnummer och inloggningsuppgifter. Utöver det har även företagshemliga uppgifter i form av patent samt framtida lanseringar stulits.

Ange till vilken grad Du instämmer eller inte instämmer med följande påståenden utifrån ovan angiven krishändelse. *

(1) instämmer inte alls, (2) instämmer inte helt, (3) varken instämmer eller instämmer inte, (4) instämmer delvis, (5) instämmer helt.

Företaget Kartula hade kunnat förhindra krisen från att inträffa.

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Företaget Kartula hade kunnat förebygga konsekvensen av cyberattacken, att känslig information läckte. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Företaget Kartula hade kunnat undvika krisen. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Företaget Kartula bör hållas ansvarig för krisen. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Företaget Kartula bör klandras för krisen. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Krisen orsakades av en svaghet i företaget Kartula. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Nedan kommer du få svara på din inställning till företaget Kartula. Markera på skalan.

Description (optional)

Min inställning till företaget Kartula är... *

	1	2	3	4	5	6	7	
Dålig	○	○	○	○	○	○	○	Bra

Min inställning till företaget Kartula är... *

	1	2	3	4	5	6	7	
Negativ	○	○	○	○	○	○	○	Positiv

Min inställning till företaget Kartula är... *

	1	2	3	4	5	6	7	
Ovänlig	○	○	○	○	○	○	○	Välvillig

Uttalande från företagen. Nedan finns ett uttalande om krisen från företaget Kartula. Efter att du har läst texten kommer du få svara på ett antal påståenden om dina åsikter om företaget.

Kära kunder,

Igår utsattes vi, Kartula AB, för en omfattande cyberattack av en hackergrupp. De stal stora mängder data i form av kunders personuppgifter och annan företagskänslig information ifrån oss.

Vid 8-tiden på morgonen upptäckte vi problem med vår hemsida. Strax därefter eskalerade attacken till en massiv spammailskampanj riktad mot våra medarbetare.

Det är med stor sorg och frustration vi konstaterar att vi fallit offer för denna attack som stod oss helt utom vår kontroll. Vi och våra kunder har blivit bestulna på en stor mängd känslig data som är av stort värde för konkurrenter eller andra intressenter och som kan vara avgörande för Kartulas framtida framgång.

Vänliga hälsningar,

Kartula AB

Ange till vilken grad Du instämmer eller inte instämmer med följande påståenden utifrån företaget Kartulas uttalande. *
(1) instämmer inte alls, (2) instämmer inte helt, (3) varken instämmer eller instämmer inte, (4) instämmer delvis, (5) instämmer helt.

Jag anser att företaget Kartula bryr sig om sina kunder.

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Jag anser att företaget Kartula är oärligt. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Jag litar **inte** på att företaget Kartula berättar sanningen om händelsen. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Jag anser att det företaget Kartula skriver är sant. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Jag anser att företaget Kartula **inte** bryr sig om välbefinnandet hos sina kunder. *

	1	2	3	4	5	
Instämmer inte alls	○	○	○	○	○	Instämmer helt

Nedan kommer du få svara på din inställning till företaget Kartula. Markera på skalan.

Description (optional)

Min inställning till företaget Kartula är... *

	1	2	3	4	5	6	7	
Dålig	○	○	○	○	○	○	○	Bra

Min inställning till företaget Kartula är... *

	1	2	3	4	5	6	7	
Negativ	○	○	○	○	○	○	○	Positiv

Min inställning till företaget Kartula är... *

	1	2	3	4	5	6	7	
Ovänlig	○	○	○	○	○	○	○	Välvillig

Observera att händelsen och företaget är fiktiva. Tack för din medverkan!

Description (optional)

9.2 Stimuli

ResponseA - Victimage and Scapegoat

Uttalande från företagen. Nedan finns ett uttalande om krisen från företaget Kartula. Efter att du har läst texten kommer du få svara på ett antal påståenden om dina åsikter om företaget.

Kära kunder,

Igår utsattes vi, Kartula AB, för en omfattande cyberattack av en hackergrupp. De stal stora mängder data i form av kunders personuppgifter och annan företagskänslig information ifrån oss.

Vid 8-tiden på morgonen upptäckte vi problem med vår hemsida. Strax därefter eskalerade attacken till en massiv spammailskampanj riktad mot våra medarbetare.

Det är med stor sorg och frustration vi konstaterar att vi fallit offer för denna attack som stod oss helt utom vår kontroll. Vi och våra kunder har blivit bestulna på en stor mängd känslig data som är av stort värde för konkurrenter eller andra intressenter och som kan vara avgörande för Kartulas framtida framgång.

Vänliga hälsningar,

Kartula AB

ResponseB - Excuse

Uttalande från företagen. Nedan finns ett uttalande om krisen från företaget Kartula. Efter att du har läst texten kommer du få svara på ett antal påståenden om dina åsikter om företaget.

Kära kunder,

Igår drabbades Kartula AB av en omfattande cyberattack utförd av en hackergrupp. Vi vill med detta uttalande informera er om den allvarliga händelsen och dess konsekvenser.

Vid 8-tiden på morgonen upptäckte vi problem med vår hemsida. Strax därefter eskalerade attacken till en massiv spammailskampanj riktad mot våra medarbetare. Attacken var omfattande och svår att kontrollera, vilket resulterade i att våra skyddåtgärder var otillräckliga. Hackarna tog sig in i våra system och stora mängder data, inklusive våra kunders personuppgifter och annan företagskänslig information, har tyvärr läckt ut. Informationen har nu spridits på flera platser på nätet.

Vi förstår att den här situationen är utmanande för de berörda kunderna, och vi gör allt vi kan för att se till att de hålls uppdaterade om de framsteg som görs. Vi beklagar de besvär som denna skadliga attack orsakar för våra kunder och alla som påverkas av den.

Med vänliga hälsningar,
Kartula AB

ResponseC - Apology, ingratiation and compensation

Uttalande från företagen. Nedan finns ett uttalande om krisen från företaget Kartula. Efter att du har läst texten kommer du få svara på ett antal påståenden om dina åsikter om företaget.

Kära kunder,

Igår drabbades Kartula AB av en omfattande cyberattack utförd av en hackergrupp. Vi vill med detta uttalande informera er om denna mycket allvarliga händelse och dess konsekvenser. Vi vill uppriktigt be om ursäkt för den oro och besvär som detta kan ha orsakat er.

Vid 8-tiden på morgonen upptäckte vi problem med vår hemsida och snabbt därpå eskalerade attacken till en omfattande spammailskampanj som riktades mot våra medarbetare. Attacken var omfattande och svår att kontrollera, vilket resulterade i att våra skyddåtgärder var otillräckliga. Hackarna tog sig in i våra system och stora mängder data, inklusive våra kunders personuppgifter och annan företagskänslig information, har tyvärr läckt ut. Informationen har nu spridits på flera platser på nätet. Vi förstår allvaret i detta och tar fullt ansvar för vårt misslyckande med att skydda er information.

Det är viktigt för oss att påminna er om det goda arbete som Kartula har utfört tidigare och vi lovar att göra allt vi kan för att återupprätta ert förtroende och fortsätta tjäna er på bästa möjliga sätt. Vi vill att ni ska veta att ni är vår högsta prioritet och att vi värdesätter den förtroendefulla relation vi har byggt upp med er under åren. För uttrycka vår tacksamhet för ert stöd och ert tålamod under denna utmanande tid kommer samtliga drabbade kunder kompenseras om en summa på 1000 kr.

Vi förstår att den här situationen är oroväckande för de berörda kunderna och vi gör allt vi kan för att se till att de hålls uppdaterade om situationens utveckling. Vi beklagar de besvär som denna skadliga attack orsakar för våra kunder och alla som påverkas av den.

Med uppriktiga ursäkter och vänliga hälsningar,
Kartula AB