Faculty of Humanities and Social Sciences

Bachelor in Global Communication

Bachelor´s Thesis

Crisis Communication in Corporate Cyberattacks

An Analysis of Reputational Risk Management

Student: **Laura Zamorano García**

Director: Prof. Sonia Aránzazu Ferruz González

Madrid, April 2026

Table of contents:

1. Introduction

1.1. Background and Relevance of the Study

The last few decades have been marked by a digital transformation and major technological advances that have reshaped economic, organizational, and social dynamics at a global scale. This evolution has also had a significant impact in the business sphere, altering the functioning of organizations and their relationship with stakeholders and other external actors. Corporations are increasingly dependent on technological infrastructures, interconnected databases, and automated internal systems. This growing dependence has led to a corresponding increase in cyber risks. In this context, cyberattacks have consolidated as a structural and recurrent threat to contemporary companies.

Recent reports point to a significant increase in cyberattacks and the associated risks. According to the Global Cybersecurity Outlook 2025 report, 72% of the surveyed organizations reported experiencing an increase in cyber risks over the last year. This rise can be explained by several interrelated factors, among them the growing use of cyberspace as a tool of geopolitical competition, the consolidation of organized crime models, and the development of technologies such as artificial intelligence that facilitate more automated and sophisticated attacks (World Economic Forum, 2025).

Cyber threats do not merely pose a pure technical risk but are established as a cross-cutting phenomenon that can affect multiple organizational levels within a corporation. In many cases, these incidents result in data breaches when sensitive, protected, and confidential information of stakeholders is accessed, viewed, or disclosed without authorization. The information stored within the corporate data systems is highly sensitive, as it may include personal data or financial information. The magnitude of these incidents extends beyond the privacy and security of users and is also reflected in their economic consequences. The average global cost of a data breach reaches 4.44 million dollars, which reflects a significant financial impact of these incidents (IBM, 2025). As a result, data breaches have become a central concern for contemporary corporations, as they increase public scrutiny and are often interpreted as an indicator of weaknesses in the organization's security infrastructure. Within this framework, stakeholders tend to reassess the competence, transparency, and integrity of the company and its technical robustness when private information is compromised, or internal vulnerabilities are disclosed. Nevertheless, although not all cyberattacks necessarily result in the leakage of personal data, empirical evidence suggests that a substantial proportion of security

incidents lead to confirmed data breaches (Verizon, 2025). Therefore, cyberattacks should not be considered isolated incidents, as they can generate systemic consequences. In this sense, cyber risk is integrated into the overall architecture of corporate risk. It must be addressed from multiple legal, strategic, and communicative perspectives, not only from a technical and technological standpoint.

From this perspective, the consequences of cyber incidents extend beyond operational disruption and financial loss. Reputational damage is among the most persistent and long-lasting effects of a cyberattack in contemporary business environments. Reputation is widely recognized as a strategic intangible asset, as its deterioration can weaken stakeholder trust and undermine corporate legitimacy in the long term. Moreover, reputation is progressively constructed through the set of evaluations that organizational audiences make regarding organizational behavior, which implies that the reputational effects of a crisis may extend beyond the incident itself (Barnett, Jermier, & Lafferty, 2006). In contexts of high media visibility, reputation also becomes one of the most vulnerable assets for organizations. As a result, cyber incidents transcend the technological domain and enter the symbolic sphere, where organizational legitimacy is created and contested.

This reputational impact is intensified by the structural characteristics of the contemporary digital environment. These systems are characterized by hyperconnectivity and informational immediacy, features that amplify the public exposure of cyberattacks and, consequently, intensify their potential reputational impact. Through social media platforms and mass media, information spreads at a vertiginous speed across interconnected networks, thereby reducing the corporation´s capacity to react and manage the initial framing of the event. Under these conditions, stakeholders make judgements regarding the degree of responsibility attributed to the organization and not solely the technical severity of the incident. These attributions play a central role in shaping reputational damage and subsequent recovery prospects. For these reasons, crisis communication is considered a core strategic domain within the corporation and constitutes a key mechanism for the protection and reconstruction of reputational capital. The effectiveness of response strategies depends on the proportional alignment between the strategy adopted and the level of reputational threat perceived by stakeholders (Coombs, 2007).

In recent years, several cyberattacks have attracted significant media attention, highlighting the potential reputational consequences that may arise from such incidents. Cyber incidents that have affected some of the world's largest corporations, such as Sony Pictures (2014), Equifax (2017), or Yahoo (2013), have demonstrated the potential reputational crisis that may result from the leakage of sensitive information or the public exposure of possible internal weaknesses in cyber management. More recently, the cyberattack targeting the corporation MGM Resorts in 2023 led to operational disruptions and generated intense media coverage, reigniting the debate about the capacity of major global corporations to adequately manage and mitigate cyber risks.

Building on these considerations, it is important to conceptualize crises arising from cyber-attacks as a communicative phenomenon and not just as merely technological incidents, as what ultimately matters is how the stakeholders interpret the event. In addition, not all corporations face the same level of reputational damage despite facing the same type of attack. Likewise, not all corporate responses are equally effective in terms of recovery. The disparities in the recovery trajectories are a direct consequence of the different strategies adopted in crisis management. Such variation depends on different factors, including the attribution of responsibility, the framing of the crisis narrative, and the corrective measures implemented, all of which contribute to different reputational outcomes. In this context, communication ceases to be understood as a merely operational reaction following the incident and is instead conceptualized as a strategic variable integrated into the system of reputational risk management. Consequently, the communication management of a cyberattack becomes part of a structured process of constructing, protecting, and ultimately reconstructing organizational legitimacy within the public sphere.

Likewise, these crises do not occur in a structural vacuum, but develop within a volatile, uncertain, complex, and ambiguous (VUCA) digital environment. This implies that information flows at an accelerated speed, making it difficult to control, and also, organizations make decisions in contexts of uncertainty where multiple actors are involved and have different interpretations of what occurred. Within this dynamic digital ecosystem, response strategies are inserted and must be analyzed in light of this context, as it conditions the possibilities for reconstructing corporate legitimacy.

The present Final Degree Project is relevant as it examines the relationship between crisis communication strategies adopted during corporate cyberattacks and the specific

configurations of their reputational effects. The increasing consolidation of reputation as a strategic asset within the broader framework of corporate risk management, combined with heightened public scrutiny in a highly mediatized environment, requires an analytical approach capable of revealing specific patterns and variations in crisis management. The examination of the factors that influence the management of crisis situations, and the resulting configurations of reputational effects, constitutes the conceptual foundation of the present research study.

1.2. Research Problem, Research Question, and Objectives

Despite the recognition of cyberattacks against corporations as critical organizational crises, the examination of the role of communicative decision-making in shaping differentiated reputational trajectories remains conceptually underdeveloped. In this regard, further analysis is needed to understand how strategic choices adopted during the response to cyber crises affect the evolution of reputational damage and recovery.

The aim of this study is not to evaluate cybersecurity infrastructures or quantify economic losses resulting from cyberattacks. Instead, it focuses on the strategic dimension of crisis communication as a structuring factor within reputational risk management processes. To address this objective, the study adopts a qualitative comparative case study design of two emblematic corporate cyber crises: Sony Pictures Entertainment (2014) and MGM Resorts International (2023). These cases serve as analytical instruments for examining differentiated communication strategies in distinct digital contexts.

Based on this framework, the main objective of the present study is to analyze the relationship between the communicative strategies employed and the reputational trajectories in corporate cyber crises.

More specifically, the research aims to:

- Identify the key communicative variables that structure reputational damage and recovery processes within corporate organizations.
- Analyze the interaction between responsibility attribution, narrative framing, and stakeholder evaluations in shaping reputational outcomes.
- Compare strategic response patterns across two differentiated digital environments in order to assess how external factors condition reputational trajectories.

In this context, the following research question guides the analysis throughout this study:

How do the crisis communication strategies adopted during corporate cyberattacks influence the configuration of reputational damage and subsequent reputational recovery processes?

In addition, the research is structured around the following sub-questions to organize the analysis systematically and coherently:

- How does the attribution of responsibility shape reputational trajectories through stakeholder evaluation during corporate cyber crises?
- How does the narrative framing influence the evolution of reputational damage and recovery?
- To what extent do the different digital contexts in which the Sony and MGM crises are unfolding condition the effectiveness of the communication strategies implemented?

2. State of the Art

Corporate crises have become a recurrent phenomenon within contemporary organizations. These events can disrupt the normal functioning and stability of organizations, placing at risk their relationships with different stakeholder groups. In the academic literature, a crisis is defined as "a specific, unexpected, and nonroutine event or series of events that create high levels of uncertainty and simultaneously present an organization with both opportunities for and threats to its high-priority goals" (Ulmer, Sellnow, & Seeger, 2018). Accordingly, events acquire the categorization of crises when they meet the criteria of surprise, threat, and urgency, in contrast to routine disruptions within normal organizational activity.

Due to the uncertainty generated by such events, organizations are often forced to act under conditions of incomplete information and high time pressure. In this setting, corporate communication acquires a central role in the crisis management process. Authors such as Valackiene (2010) emphasize the strategic management function performed by corporate communication, as it allows the coordination of the different organizational actors involved in the crisis and ensures the flow of information between internal and external publics. Moreover, in order to provide truthful information to the audience and minimize distortions in the interpretation of the event, organizational leadership must cooperate with the media. In doing so, the uncertainty experienced by

affected stakeholders can be reduced, thereby preserving stakeholder trust and protecting organizational legitimacy. Therefore, effective and active communication based on transparency fosters a responsible corporate culture and reduces one of the elements that most complicate crisis management, namely uncertainty (Valackiene, 2010).

In the current digital environment, companies are increasingly dependent on digital technologies for the development of their operations. Although this technological transformation offers important opportunities in terms of efficiency and innovation, it also increases their exposure to cyber threats and malicious intrusions against their systems. As a consequence, corporations become intrinsically more vulnerable to this type of threat. This makes it necessary to define the concept in order to facilitate its understanding within the analysis of contemporary corporate crises. Cyberattacks can be defined as malicious actions carried out through cyberspace that target the digital systems of an organization to interrupt, disable, or destroy information infrastructures, illegally controlling computational environments or compromising data integrity through the access, manipulation, or extraction of sensitive information (National Institute of Standards and Technology, 2019).

Recent literature (Kamiya et al., 2021; Perera et al., 2022; Toma et al., 2023) demonstrates that these incidents are no longer interpreted solely as information security breaches but are increasingly conceptualized as events capable of generating significant disruptions across multiple dimensions of organizational functioning, with shareholder losses far exceeding direct costs. Several studies underline that such incidents may generate major financial losses associated with system recovery, legal costs, and other response measures, as well as operational disruptions that threaten business continuity. Nevertheless, one of the most relevant effects and one that raises increasing concerns among contemporary corporations relates to their reputational implications. In particular, Fotis (2024) identifies reputational damage as one of the most significant indirect economic impacts of cyber incidents, as it can erode the trust of customers and investors and affect the positioning of the company in the market. In his analysis, he points out that companies that have suffered a cyberattack experience, on average, an approximate decrease of 10% in their customer base during the first year following the incident (Fotis, 2024). Within this context, cyberattacks are increasingly analyzed in the academic literature as complex organizational crises whose management requires not only technical

responses, but also strategic communication efforts aimed at managing the public perception of the event and protecting corporate reputation.

Given the growing relevance of reputation in this type of crisis, it becomes necessary to clarify what is meant by corporate reputation. The notion of reputation has at times been associated with merely intuitive and general terms, such as a company´s image or prestige. Nonetheless, to avoid vague interpretations, it is essential to conceptually delimit it. From an academic perspective, Barnett, Jermier, and Lafferty (2006) define corporate reputation as "observers' collective judgments of a corporation based on assessments of the financial, social, and environmental impacts attributed to the corporation over time" (Barnett et al., 2006, p. 33). This highlights its evaluative and cumulative character, since reputation is progressively configured through the aggregate assessments made by different stakeholders regarding organizational behavior. Based on this definition, reputational damage may lead to the erosion of an intangible asset that has been progressively built over time, rather than merely constituting a simple temporary alteration of the corporation´s image. Because reputation strongly influences stakeholder groups such as investors, customers, and regulators, its deterioration may affect the organization's ability to recover from crises and maintain its institutional legitimacy.

Taken together, the reviewed literature shows that cyberattacks have consolidated as a particular type of organizational crisis with significant implications for corporate reputation and stakeholder relationships. However, although numerous studies have analyzed the economic, operational, and reputational consequences of these incidents, the specific role played by communication strategies in shaping stakeholders´ interpretations of such crises has received less attention. In this regard, it is particularly relevant to analyze how the communicative decisions adopted by organizations during a cyberattack may influence the interpretation that stakeholders make of the event and, consequently, the evolution of reputational damage and the possibilities for restoring trust. From this standpoint, the present study is situated at the intersection between crisis communication and reputational risk management, examining how communicative strategies adopted during corporate cyberattacks influence reputational outcomes in the contemporary digital environment.

3. Theoretical framework

The present study draws on three complementary theoretical perspectives within the field of crisis communication to analyze the communication strategies adopted during selected corporate cyberattacks. First, the Situational Crisis Communication Theory (Coombs, 2007) provides an analytical framework to understand how stakeholders attribute responsibility to corporations during crisis contexts and how these attributions shape the perceived level of reputational threat. Second, the Image Repair Theory (Benoit, 1997) offers conceptual tools to examine the discursive and communicative strategies that organizations employ to protect, defend, and reconstruct their reputation after a damaging event. Finally, the analysis is complemented by the concept of corporate reputation, which allows the examination of the reputational implications resulting from the communicative management of the crisis.

3.1 Situational Crisis Communication Theory (SCCT)

Given this focus on reputation in organizational crises, Attribution Theory (Coombs, 2007) stands out within the academic literature as a fundamental theoretical framework for understanding the configuration of reputational damage during a crisis. This theory starts from the premise that human beings act as "naïve psychologists" who, in a systematic and largely unconscious manner, seek to identify the causes of incidents, as well as to understand the behavior of others in order to make sense of the social environment. When transferred to the organizational sphere, this logic makes it possible to analyze how stakeholders interpret a crisis and evaluate the degree of responsibility of the corporation involved.

In this process, stakeholders assess different causal dimensions that shape this perception of the degree of responsibility attributed. Three main dimensions are distinguished. First, the locus of control or causality, which refers to the perceived origin of the crisis. If the cause is attributed to internal factors of the organization, greater responsibility is attributed to it. Conversely, when the crisis is perceived as resulting from an external factor beyond the organization's control, it is typically classified within the "victim cluster," granting it a lower level of attributed responsibility. On the other hand, the degree of controllability is evaluated. Even when the origin of the crisis is external, audiences assess the factor of negligence to determine whether the organization had the competence or control to prevent the damage caused, in other words, to determine if the event was foreseeable or inevitable. Finally, the stability of the causal factors is considered, which

refers to whether the cause of the crisis is perceived as a recurrent (stable) or, alternatively, a unique and temporary incident, in which case it is classified as unstable. To do this, stakeholders often rely on the organization's previous performance and crisis history. When it is interpreted as a systemic pattern or an ongoing unresolved problem, the degree of blame tends to increase. This attribution process can also affect the effectiveness of crisis communication strategies, as messages from "responsible" organization are received with greater skepticism by the audience. Taken together, these evaluative dimensions enable stakeholders to determine whether the cause was internal or external, recurrent or exceptional, and controllable or inevitable (Coombs, 2007).

Through this interpretative process, different levels of perceived responsibility are configured, which are established as a mediating cognitive variable between the disruptive event and its reputational consequences (Coombs, 2007). The attribution of responsibility, therefore, constitutes the mechanism through which the magnitude of reputational threat is constructed, conditioning the subsequent type of organizational response. Thus, the view that attribution is merely a retrospective evaluation of the event is abandoned.

The explanatory relevance of the attribution model is reinforced by the empirical evidence provided by Coombs and Holladay (2005), whose study systematically examined stakeholder reactions to organizational crisis. This experimental design, used to systematically analyze public reactions, is causal and theory-testing rather than speculative, unlike other studies. The study tests the existence of a consistent negative relationship between attributed responsibility and corporate reputation, demonstrating that perceived responsibility not only affects the subsequent reputational evaluation but also activates differentiated emotional responses that directly influence stakeholders´ behavioral intentions. In this context, stakeholder emotions operate as a critical mediator between responsibility attribution and behavioral intentions, functioning on a parallel track to reputational evaluations in shaping stakeholder responses.

If they determine that the organization is causally implicated and that it could have avoided the crisis or acted negligently, the evaluation of reputation is significantly eroded. The greater the responsibility attributed, the lower the post-crisis reputation score. In particular, high levels of responsibility translate into the activation of anger and, in some cases, schadenfreude, which means drawing pleasure from the pain of others (Coombs, 2007). This leads to subsequent harmful behavior, such as withdrawal of support or

negative word-of-mouth communication, while low levels of responsibility generate an increase in sympathy and may foster supportive behavioral intentions toward the corporation. In this sense, the empirical literature consolidates an explanatory architecture in which attribution, affect, and reputational evaluation are directly interrelated within the same interpretative process (Coombs & Holladay, 2005). These findings provide empirical support for an attribution-based crisis communication model, such as Situational Crisis Communication Theory (SCCT), which relies on stakeholders´ perception to select appropriate crisis response strategies.

Building upon this empirically reinforced model, the crisis communication research has developed theoretical frameworks that systematize the relationship between perceived responsibility and the selection of appropriate organizational response strategies. In this context, integrating Attribution Theory into its analytical structure, the Situational Crisis Communication Theory (SCCT) stands out as one of the most influential models in the field. It was developed with the objective of anticipating stakeholder reactions and thereby maximizing the protection of the organization´s reputation. To this end, it established a typology organized into three main clusters, which operate as classification frameworks according to the level of responsibility that the public is likely to attribute to the organization. As discussed above, crises perceived as resulting from external factors are typically categorized within the victim cluster, where the organization is also considered a victim of the event and responsibility attributions are minimal. Similarly, the accidental cluster compromises crises that arise from unintentional or uncontrollable organizational actions, such as technical-error accidents, and therefore generate relatively weak attributions of responsibility. In contrast, the intentional or preventable cluster involves purposeful actions or gross negligence, such as management misconduct or human- error accidents, and consequently produces the strongest attributions of responsibility and the highest level of reputational threat (Coombs, 2007)

The contribution of the model lies in its approach, focused not only on cataloguing response strategies but on establishing a formal link between contextual variables and strategic adequacy. In this sense, SCCT prescribes that organizations should align their crisis communication strategies and responses to the reputational threat level. Firstly, deny strategies and tactics like scapegoating are primarily recommended for rumors or challenges that seek to break the connection between the organization and the crisis. Then, adopting a diminished posture is recommended when the organization seeks to reduce the

perceived gravity of the crisis or its control over it. It is considered appropriate for crises located within the accidental cluster and includes responses such as excuses or justifications. In contrast, rebuild strategies, such as apology or compensation, represent the most accommodative response and are required when the organization is perceived as highly responsible for the event. Finally, bolstering strategies may be used as supplementary responses to reinforce positive perceptions by reminding stakeholders of the organization's past good actions or emphasizing that the organization has also been affected by the crisis.

Moreover, SCCT argues that the level of reputational threat does not depend exclusively on the initial crisis type. It is also intensified by situational variables such as the organization's crisis history and its prior relational reputation since a record of similar crises or a previously negative relationship with stakeholders may weaken the reputational buffer available to the organization. In addition, this model incorporates normative considerations, prioritizing the provision of instructive and adaptive information that seeks to protect stakeholders' safety. In other words, it introduced an ethical hierarchy into the crisis communication management (Coombs, 2007).

3.2 Image Repair Theory (IRT)

Alongside the attribution-based perspective outlined above, Image Repair Theory (Benoit, 1997) constitutes one of the foundational models in crisis communication research. This theory is situated within the theoretical tradition of corporate apologia, in which organizations confront public criticism by constructing persuasive responses designed to articulate a convincing alternative narrative that protects the institutional image, and the theory of accounts, understood as justificatory explanations that actors present to protect their reputation in the face of criticism and rationalize contested conduct (Ulmer et al., 2018). These theories serve as the starting point for IRT, which maintains as its fundamental premise the assumption that crisis communication is a persuasive discourse designed to protect the most valuable asset of an organization: its image. Moreover, this theory holds that a crisis only occurs if the organization is considered responsible for an action and if that action is offensive to the audience. Importantly, Benoit emphasizes that the key issue is whether the relevant audience perceives the organization as responsible for the offensive act. Based on this approach, Image Repair Theory (IRT) systematizes a set of discursive strategies to restore organizational

legitimacy by identifying the main rhetorical alternatives available when facing an accusation (Benoit, 1997).

Within this framework, an image threat arises from a persuasive attack when two necessary conditions are met. On the one hand, there must be an attribution of responsibility to the organization for a specific action, whether through acts carried out, permitted, ordered, or even through omissions, and on the other hand, that action must be perceived as offensive or harmful by a relevant audience. If the act is not perceived as negative, the reputation is not at risk. In this sense, this theory maintains that perceptions are more important than reality. Therefore, corporate crisis communication strategies must be persuasive discourses designed to align stakeholders' perceptions with the desired image and restore legitimacy (Benoit, 1997; Benoit, 2013). On this basis, IRT provides five general categories of communication strategies that must be employed when reputation is threatened.

First, the strategy of denial seeks to eliminate the link between the organization and the offensive act, either through the simple and direct denial of the event or through shifting the blame to another actor. Second, evasion of responsibility is used when the organization cannot deny its involvement and therefore attempts to reduce the degree of attributed responsibility by arguing that the event resulted from factors beyond its control, such as accidents, provocations, or defeasibility, which is when there was a lack of information. Third, the strategy of reducing offensiveness seeks to decrease the perceived severity of the act through different discursive tactics, such as bolstering, which emphasizes the organization´s positive or past actions, minimizing the harm caused, differentiating the act within a broader comparative framework so that it appears less serious, or attacking the accuser to undermine their credibility, among others. Fourth, corrective action consists of committing to resolve the problem and adopting measures that prevent its repetition in the future. Finally, the strategy of mortification involves fully admitting responsibility for the offensive act, explicitly apologizing, and expressing remorse. Benoit further argues that the effectiveness of these strategies depends on their internal consistency, as contradictory combinations may weaken the credibility of the response and weaken its capacity to restore organizational reputation (Benoit, 1997).

However, unlike the attributional model developed later, IRT does not establish a formal link between situational variables and strategic adequacy grounded in empirical evidence. Its formulation is supported by retrospective case analysis, focused on identifying

recurrent patterns in organizational responses. In this sense, this theory does not articulate a predictive framework to anticipate reactions to crises, but rather its orientation is predominantly descriptive and qualitative, centered on identifying what to say, rather than specifying why and when to say something and adopt a particular strategy, as is done in SCCT. Therefore, the comparison between Benoit's theory (IRT) and the later theory developed by Coombs (SCCT) demonstrates a methodological transformation in crisis communication that evolves toward more explanatory and prescriptive models based on empirical testing.

Despite these limitations, Image Repair Theory remains a valuable framework for identifying the rhetorical strategies organizations employ when responding to reputational crises.

3.3 Corporate Reputation and Reputational Risk

Within crisis communication research, crises are also understood as processes of meaning-making, which is why communication and storytelling gain relevance within this theoretical approach. In this sense, crises often emerge from an expectations gap, which occurs when stakeholders´ expectations about organizational behavior do not coincide with the information available about the organization´s actions (Ulmer et al., 2018). Under such circumstances, corporations seek to preserve their bases of legitimacy, as these may be damaged during crisis contexts and, in some cases, may even jeopardize the corporation´s continuity.

From this relational perspective, reputation becomes a strategic variable rather than a mere collateral consequence of the event. Within this framework, organizational reputation is conceptualized as the central intangible asset at stake in these disruptive events.

Reputational threat is defined as the level of potential damage that a crisis inflicts on an organization´s reputation if the measures taken fail to mitigate the negative perceptions generated among stakeholders (Coombs, 2007). This threat is not a static or isolated factor but conditioned by situational variables such as the degree of responsibility attributed to the organization, its crisis history, and its prior relational reputation. From this perspective, corporate reputation can be understood as capital accumulated over time, conceptualized as "reputational capital." Moreover, in crisis contexts, a favorable prior reputation may function as a reputational buffer, allowing the organization to draw on

previously accumulated capital to absorb the damage caused by the crisis, thereby facilitating a faster recovery (Coombs, 2007).

Importantly, it is important to consider that many foundational models of crisis communication were developed prior to the current digital environment characterized by hyperconnectivity and informational immediacy. Empirical evidence suggests that contemporary media ecosystems influence perceptions of reputational blame, intensifying and reconfiguring traditional attributional processes. Under these conditions, patterns of responsibility attribution may differ from the assumptions formulated in earlier theoretical frameworks. Jørgensen (2018) suggests that in technology-related crises, such as corporate cyberattacks, stakeholders tend to attribute greater internal responsibility to the organizations than predicted by traditional models such as SCCT, which have often classified these events within the "victim cluster." In such situations, perceived deficiencies in cybersecurity protection may be interpreted as indicators of organizational negligence, thereby intensifying reputational threat. This perspective highlights the relevance of examining corporate cyberattacks within the broader domain of crisis communication research (Jørgensen, 2018).

4. Methodology

4.1. Research Design and Case Selection Criteria

The present study adopts a qualitative comparative case study design to examine the relationship between crisis communication strategies utilized during corporate cyberattacks and reputational outcomes. Case study methodology is appropriate for examining contemporary social phenomena within their real-world environment, particularly when the boundaries between the phenomenon and its context are closely interconnected (Yin, 2018). In this context, the case study approach allows for an in-depth examination of crisis communication processes within specific organizational and media environments.

This study is guided by the theoretical framework outlined in the prior chapter, which identified the dimensions of analysis for examining the selected case studies.

The empirical component of the research consists of a comparative case study approach of two different corporate cyber crises: Sony Pictures Entertainment (2014) and MGM Resorts International (2023). These cases were selected according to four different criteria. First, their high public visibility and extensive media coverage. Second, their

analytical relevance for examining crisis communication in corporate cyber incidents. Then, the significant reputational exposure generated by these incidents. Lastly, separated by nearly a decade, which allows us to explore how crisis communication strategies evolve within changing digital environments.

The Sony Pictures case (2014) was selected because it constitutes one of the earliest and most high-profile corporate cyberattacks of the digital era. This case received extensive international media coverage and generated significant political and public debate. The attack involved data theft and system destruction. In addition, it was later formally linked by US authorities to North Korea, so the incident transcended the corporate domain, introducing a geopolitical dimension as well as increasing its visibility (Federal Bureau of Investigation, 2014).

On the other hand, the MGM Resorts case (2023) was selected as a more recent example of a corporate cyber crisis that unfolded in a highly interconnected digital environment. The cyberattack affected the systems and temporarily disrupted hotel and casino operations, illustrating the potential impact of these incidents on large corporations (Schrader, 2025).

4.2. Data Sources and Analytical Framework

The empirical analysis employs a combination of primary and secondary sources regarding the selected cyber incidents. Primary sources consist of the official corporate communications issued by the organizations during the crisis. This includes press releases, public statements, and other responses issued by the organizations published through corporate channels. It provides direct insight into how the corporation framed the incident and communicated its responses.

The primary sources are complemented by secondary sources, including media coverage and other publicly available information related to the cyber incident. In this context, media sources are used to contextualize the crisis and to illustrate its public dimension within the digital information environment, rather than constituting a primary object of systematic analysis. The selection of sources prioritizes academic literature and institutional reports, while media sources are incorporated exclusively for contextual and illustrative purposes.

The analysis is conducted through a qualitative examination of the content of these materials in order to identify patterns in the communicative responses adopted by the corporations.

4.3. Statement on the Use of Artificial Intelligence

In preparing this Final Degree Project, artificial intelligence tools such as ChatGPT or DeepL were used instrumentally, primarily for tasks related to language translation, stylistic revision, and structural organization of the text. These tools were occasionally employed to translate certain sections into English and to improve the clarity, coherence, and overall organization of the written content.

All the outputs generated with these tools were critically reviewed, revised, and adapted by the author. Under no circumstances did the use of artificial intelligence substitute the author´s own research, analysis, or writing. The author is fully responsible for the content, arguments, and conclusions presented in this work.

5. Case Analysis

This chapter empirically analyzes the two selected cases: Sony Pictures Entertainment (2014) and MGM Resorts International (2023). The cases are examined through a qualitative analysis of the communication strategies adopted by the organizations during the crisis and their potential reputational implications.

The analysis follows the analytical framework established in the theoretical chapter, focusing on three main dimensions: the context of the cyber incident, the corporate communication response, and the theoretical interpretation of the strategies implemented.

5.1. Sony Pictures Entertainment (2014)

5.1.1 Context and Overview of the Cyberattack

The 2014 cyberattack against Sony Pictures Entertainment is widely regarded as a landmark event in the history of cybersecurity and in the dynamics of international geopolitics, due to its magnitude, political implications, and global media impact. The incident is particularly relevant because it demonstrates that private corporations could become direct targets of geopolitical conflicts. Unlike other attacks directed at private corporations motivated by economic incentives or industrial espionage, this one was interpreted as an act of political coercion and deterrence (FBI, 2014).

The direct trigger of the attack was the content of the film *The Interview*, a satirical comedy in which the CIA recruits a television host and his producer to assassinate the North Korean leader, Kim Jong-un. After the trailer was released, the ambassador of North Korea sent a letter to the Secretary-General of the United Nations condemning the film as "the most blatant act of terrorism and war" (Steinberg et al., 2021, p.4). The act represented a significant threat to the Pyongyang regime, since in North Korean political culture, the authority of the Kim family occupies a central role in the ideological structure of the state. Consequently, satire directed at the leader can be interpreted as a symbolic attack on the nation's sovereignty. Furthermore, the film was considered by the regime a potential threat because they feared that it could be leaked and circulated through the black-market channels within the country, encouraging citizens to question the official state narrative and prompting social dissent. This context contributed to building a political rhetoric that was later used to justify the cyberattack (DeSimone & Horton, 2017).

Although the cyberattack became publicly known in November 2014, intrusions into Sony's systems had begun months earlier. Through spear-phishing techniques (digital fraud), the attackers managed to infiltrate the corporate network in September and obtain employee access credentials. This internal information enabled them to operate within the company's digital infrastructure for months before executing the visible and destructive phase of the attack (FBI, 2014). Among the leaked materials, the attackers exfiltrated sensitive information, including internal executive emails, financial documents, and copies of unreleased films, thereby compromising the company's intellectual property. The publication of these materials generated extensive media coverage because the emails contained important internal decisions within Sony, which amplified the reputational impact of the incident (Laughland & Rushe, 2014).

On 24 November 2014, Sony employees discovered the breach when computer screens displayed an image of a red skeleton, accompanied by the message "Hacked by #GOP." The perpetrators, who belonged to a group called Guardians of Peace, threatened to publish all stolen data if their demands were not met. Initially, they demanded financial compensation for the alleged damages caused, and later these demands evolved toward the cancellation of the film's release, in addition to threatening physical attacks similar to those of 11 September 2001 (Laughland & Rushe, 2014).

Subsequent investigations revealed that the cyberattack combined destructive malware with the massive theft of information. According to the FBI report, the attackers deployed malware that erased data and corrupted the hard drives of the affected devices. As a consequence, Sony was forced to disconnect its global corporate network to contain the intrusion, which disrupted the corporation´s operations (FBI, 2014).

Following further investigations that identified technical similarities with tools previously used by North Korean actors, the US government formally attributed responsibility to the North Korean regime on 19 December 2014 through an official statement issued by the Federal Bureau of Investigation. At the time, the American President, Barack Obama, stated that the attack constituted an attempt to suppress citizens' right to express themselves freely, thereby attacking a fundamental human right: freedom of expression. This situation generated an intense public debate about the possibility that a foreign actor could influence the distribution of cultural content in the United States, since several cinema chains decided to cancel the screening of the film due to the fear generated by the hackers' threats. Finally, Sony decided to release the film on 25 December 2014 through a limited theatrical release and digital platforms (FBI, 2014; Laughland & Rushe, 2014).

Taken together, these events transformed the cyberattack against Sony Pictures Entertainment into one of the most emblematic cases of corporate cyber crises of the last decade. The case highlighted the complexity that digital crises can acquire when technological, media, and political factors converge. From this perspective, it becomes relevant to analyze how the company communicatively managed the crisis and the strategies it adopted in response to the cyberattack.

5.1.2 Corporate Response and Crisis Communication Strategy

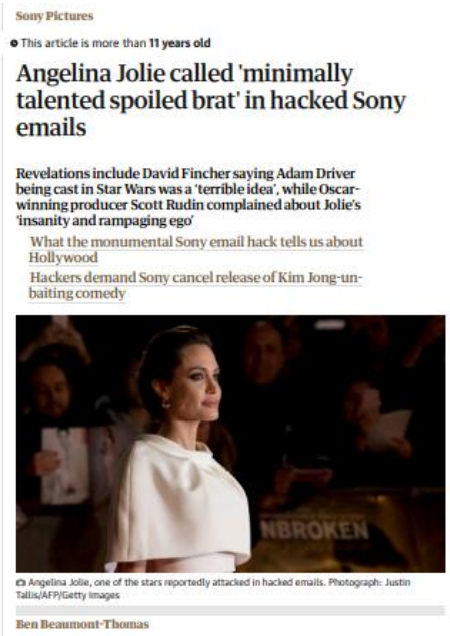
This section analyzes the corporate communication strategy adopted by Sony Pictures Entertainment, focusing on how the company reframed the crisis narrative to mitigate reputational damage.

Following the public disclosure of the incident on November 24, 2014, Sony faced a highly complex crisis context, as it was not only a technological crisis, but it quickly acquired a reputational and geopolitical dimension. In this scenario, the corporation had little time to construct a narrative and manage a strategic response appropriate to the situation in order to mitigate the potential reputational consequences derived from the public exposure.

In a first instance, the corporate response was dominated by a logic of operational containment. The attackers had full control of the company's digital environment, which severely constrained Sony's ability to articulate an immediate communicative response. This initial reaction was rapid and drastic, materializing in a "shutdown" of the computer systems, which were deactivated in order to contain the spread of the virus. Sony was forced to operate through manual procedures during the first weeks, being thrown back to the Betamax era. The corporation returned to using analog technologies such as fax machines, the issuing of paper checks, and communication had to be carried out face-to-face, which illustrates the total technological collapse caused by the cyberattack (Steinberg, Stepan, & Neary, 2021). This shows how, during the first phase, the corporate response was predominantly preventive, oriented toward operational survival, and dominated by a low-profile communicative strategy of victimization, in which the company presented itself as the victim of a highly sophisticated attack.

However, at the beginning, the attackers demanded financial compensation and threatened the publication of the stolen information but did not explicitly mention the film *The Interview* as the motive behind the attack. This ambiguity meant that Sony could not construct an effective communication strategy from the first day, nor clearly explain to stakeholders the origin or logic of the attack. As a consequence, during those first weeks, a climate of fear and uncertainty emerged within the company and in the media environment, further complicating crisis management. The situation worsened with the leak of internal emails containing complaints and disparaging comments from senior executives of the company toward Hollywood stars or relevant public figures in the international arena, such as Obama, about whom racist jokes were made (Steinberg et al., 2021; Rushe & Laughland, 2014). From that moment onwards, the crisis turned into a reputational scandal that directly affected the relationship of trust between the studio and creative talent, a key stakeholder group whose trust contributes to the legitimacy of the studio within the Hollywood ecosystem. This media scandal pressured the company to redefine its communication strategy.

This transformation of the crisis into a reputational scandal is clearly reflected in the media coverage of the incident, as illustrated in Figure 1.



Sony Pictures

This article is more than 11 years old

Angelina Jolie called 'minimally talented spoiled brat' in hacked Sony emails

Revelations include David Fincher saying Adam Driver being cast in Star Wars was a 'terrible idea', while Oscar-winning producer Scott Rudin complained about Jolie's 'insanity and rampaging ego'

What the monumental Sony email hack tells us about Hollywood

Hackers demand Sony cancel release of Kim Jong-un-baiting comedy

Angelina Jolie, one of the stars reportedly attacked in hacked emails. Photograph: Justin Tallis/AFP/Getty Images

Ben Beaumont-Thomas

Figure 1

Media coverage of the Sony Pictures email leak highlighting the reputational impact of internal communications on relationships with Hollywood talent.

Source: Beaumont-Thomas, 2014.

From a discursive perspective, one of the key moments within this crisis management occurred during the climax of the conflict, when, following the threats of physical violence issued by the attackers, the CEO of Sony Pictures Entertainment, Michael Lynton, released an official statement announcing the cancellation of the film's theatrical release. On December 17, 2014, the company declared the following: *"*In light of the decision by the majority of our exhibitors not to show *The Interview*, we have decided not to move forward with the planned December 25 theatrical release*"* (Rushe & Laughland, 2014).

This statement represents a strategic turning point in the communicative management of the crisis. The way in which the corporate message is formulated introduces a mechanism of externalization of responsibility. By stating "in light of the decision by the majority of our exhibitors…", the corporation is shifting the agency of cancelling the release of the film to an external actor, in this case, the cinema owners who, after receiving the threats from GOP, decided not to screen it. This discursive shift reflects a change in the corporate narrative in which the logic of crisis management extends beyond cybersecurity concerns and moves toward the management of the cultural product itself. However, despite this shift in the narrative, the corporate response conveys a position of strategic capitulation,

which consisted of a series of concessions, such as the cancellation of the release (Steinberg et al., 2021). In addition, they mentioned that they did not even have further release plans for the film in any format (Rushe & Laughland, 2014).

Nevertheless, this decision generated considerable controversy and was strongly criticized by figures such as Senator John McCain, who argued that it effectively meant yielding to acts of cyberterrorism and could encourage other malicious actors to use cyberspace offensively. Other figures in the industry, such as Steven Carell, expressed their disappointment, stating that "it was a sad day for creative expression" (Rushe & Laughland, 2014), as his film set in North Korea had also been cancelled for fear of a reaction similar to that surrounding *The Interview*. On the other hand, U.S. President Barack Obama publicly expressed his disappointment with the decision to cancel the film, after having attributed responsibility for the attack to North Korea and assuring that the United States would respond proportionally. Therefore, these reactions contributed to transforming the corporate crisis into an issue framed within a broader debate of national pride and national security, thereby increasing public pressure on Sony to reconsider its decision and adopt a different narrative (Rushe & Laughland, 2014).

Following this media pressure, the corporate narrative of Sony Pictures was redefined and shifted toward a more active communicative response. From that moment onwards, official statements began to reformulate the meaning of the incident, presenting it as a conflict linked to the defense of fundamental values and not solely as a security incident. On December 23, 2014, the CEO, Michael Lynton, issued an official statement in which he affirmed that: *"*We have never given up on releasing *The Interview* and we are excited that our movie will be in a number of theaters on Christmas Day." ″At the same time, we are continuing our efforts to secure more platforms and more theaters so that this movie reaches the largest possible audience.″ (Sony Pictures Entertainment, 2014a). This statement seeks to erase the image of surrender that was projected when the company announced that there were no further plans for the release of the film. The earlier strategic capitulation was therefore rhetorically rectified by asserting that Sony never abandoned the planned release strategy.

At the same time, the company seeks to rebuild the relationship with one of its most important stakeholders, namely the creative talent of Hollywood, and to reconstruct its reputation within the ecosystem of the industry through the following corporate message:

> I want to thank our talent on *The Interview* and our employees, who have worked tirelessly through the many challenges we have all faced over the last month. While we hope this is only the first step of the film's release, we are proud to make it available to the public and to have stood up to those who attempted to suppress free speech (Sony Pictures Entertainment, 2014a).

This discursive repositioning was accompanied by a broader normative framing that linked the release of the film to the defense of freedom of expression: "(...) It was essential for our studio to release this movie, especially given the assault upon our business and our employees by those who wanted to stop free speech (...)" and " While we hope this is only the first step of the film's release, we are proud to make it available to the public and to have stood up to those who attempted to suppress free speech." (Sony Pictures Entertainment, 2014b)

Through these statements, Sony sought to politicize its corporate response in order to protect its image within the industry and to position itself as a defender of freedom of expression, which is a foundational value within the American democratic culture. The narrative created played the role of a reputational shield and allowed the company to divert attention from its negligence, which consisted of the underestimation of cyber risk (Steinberg et al., 2021), while also counteracting the impact of the leaked information by focusing the audience's attention on its defence of the fundamental right of freedom of speech. Finally, the company sought to construct a narrative of resistance through the declaration: "I'm proud our fight was not for nothing and that cyber criminals were not able to silence us." (Sony Pictures Entertainment, 2014b). In this framing, the corporation portrays itself as an actor that had not yielded to the threats and had fought against the cyber attackers until obtaining a symbolic victory in the crisis, thereby reinforcing its legitimacy before public opinion.

5.1.3 Theoretical Interpretation and Reputational Implications

While the previous section examined the corporate response from an empirical and discursive perspective, based on that analysis, it is possible to interpret the case of Sony Pictures Entertainment (2014) in light of the theoretical framework described in Chapter 3. The application of crisis communication theories to the cyberattack makes it possible to examine how the corporation manages its most valuable asset, reputation.

From the perspective of Situational Crisis Communication Theory (SCCT), the case allows for an analysis of how the stakeholders' attributions of responsibility shape the configuration of reputational threat during a crisis. According to this model, in crises, corporations must follow a structured process to protect their reputation. This process begins with a primary ethical responsibility and is followed by two analytical steps: determining the initial level of responsibility in order to identify what type of crisis the organization is facing, and subsequently evaluating potential intensifying factors.

First, Sony did not carry out the so-called step 0 of SCCT, according to which organizations must give absolute priority to protecting stakeholders by providing instructive and adaptive information before adopting strategies to protect the company's reputation. Sony did not immediately notify current or former employees about the incident, which prevented those affected from taking preventive measures to protect themselves against physical or financial threats such as identity theft. This way of acting began to damage the corporate image and contributed to a loss of legitimacy. As a consequence, the company also faced a multimillion-dollar class action lawsuit filed by former employees (Coombs, 2007; DeSimone & Horton, 2017).

Secondly, according to this theory, the level of attribution of responsibility to the company should be determined. Sony positioned itself within the victim cluster by categorizing the cyberattack as an act of external malevolence or terrorism by a state actor. By using the strategy of victimization, the corporation sought to present itself as the target of an uncontrollable attack in order to receive a low level of attribution of responsibility and result in a mild reputational threat. However, despite having correctly constructed that idea of victimization, the corporation maintained this narrative without acknowledging its own internal technical vulnerabilities. The failure to recognize potential internal weaknesses reduced the credibility of the organization among stakeholders, which contributed to intensifying the reputational impact of the incident (Coombs, 2007; DeSimone & Horton, 2017).

Subsequently, Sony should have properly evaluated the crisis-intensifying factors since these can multiply the reputational threat. According to SCCT, these factors are mainly crisis history and prior relational reputation (Coombs, 2007). On the one hand, Sony already had a recurrent crisis history, having suffered a massive hack of the PlayStation Network in 2011. In addition, the hacker community had coined the term "Sownage" to mock the constant cyber humiliations suffered by the company. This prior history

weakened the reputational buffer available to the organization and increased the likelihood of being attributed with a higher responsibility. On the other hand, its relationship with stakeholders, understood as prior relational reputation, was not favorable due to its combative and negligent stance in previous controversies. The corporation had already faced scandals such as the Rootkit case (2005), in which it installed hidden software on 20 million CDs to prevent piracy, violating the trust of its customers. Likewise, during the course of the crisis, information was leaked about technical vulnerabilities, such as the lack of investment in cybersecurity due to cost-saving priorities or the use of extremely simple passwords such as "sony12345". As a consequence, a significant discrepancy emerged between the corporate narrative of victimization and the public interpretation of the event. This gap favored the progressive shift in framing from a victim crisis toward an interpretation closer to the preventable cluster, in which stakeholders perceive the crisis as something that could have been avoided. The shift in crisis framing intensified the reputational threat and illustrates how, in cyber crises, initial crisis categorizations may rapidly evolve when new information questions the organizational competence in managing security risks (Steinberg et al., 2021; Coombs, 2007).

This shift can also be understood in terms of the causal dimensions defined by Attribution Theory. First, although the triggering cause of the incident was external, the leakage of evidence of negligence in cybersecurity practices led stakeholders to attribute an internal locus of causality to the corporation. Second, the crisis came to be perceived as highly controllable, since it was revealed that Sony had ignored prior warnings about their technical vulnerabilities. Finally, the accumulation of security vulnerabilities in the company has led to the perception of the cause of the cyberattack as relatively stable, rather than being understood as an isolated event (Ulmer et al., 2018).

Beyond the attribution of responsibility, Sony's communicative response can also be interpreted through Image Repair Theory (Benoit, 1997), which makes it possible to analyze the discursive strategies used by Sony to restore its legitimacy once its reputation was already damaged. According to this theory, for a corporation to initiate an image repair process, it must be perceived as responsible for the act, and the act must be considered offensive by a relevant audience. Several of the statements analyzed in the previous section reflect the use of different strategies to improve reputation during the cyber crisis. First, the company resorted to strategies of evasion of responsibility,

especially through defeasibility, by claiming a lack of ability to prevent the highly sophisticated attack. Furthermore, by presenting the attack as being carried out by another State, North Korea, the corporation sought to persuade audiences that no preventive measure would have been sufficient (DeSimone & Horton, 2017).

Likewise, to shift the blame, Sony suggested in its communications that the cancellation of the film had been caused by third parties. The category most frequently used in its statements from December 2014 onwards was the reduction of offensiveness, particularly through strategies of bolstering and transcendence. Sony attempted to reinforce positive public sentiment by emphasizing its resilience, stating that it had never given up on the release of *The Interview*. The strategy of transcendence was applied by framing the film as a battle for freedom of expression, thereby elevating the issue to a normative level so that the technical negligence would go unnoticed (Sony Pictures Entertainment, 2014a; Sony Pictures Entertainment, 2014b; Benoit, 1997). Alongside this, the company incorporated elements of corrective action by promising the improvements to its security infrastructure so that the public would trust that the situation would not occur again. However, Sony Pictures Entertainment avoided using the strategy of mortification regarding the technical incident itself in order to limit potential legal consequences, although it did issue apologies for the content of the leaked emails. Taken together, these corporate responses appeared partially inconsistent since internal practices contradicted the narrative that Sony was merely the victim of an external actor and a defender of freedom of expression (Benoit, 1997; Jørgensen, 2018).

Finally, the Sony case illustrates how a cyber crisis can translate into a reputational risk of great magnitude when communicative management fails to neutralize negative stakeholder perception. In this sense, the crisis transcended the technical dimension of the cyberattack to become a direct threat to organizational legitimacy and to the overall reputational evaluation of the company by its stakeholders (Barnett, Jermier & Lafferty, 2006).

5.2. MGM Resorts International (2023)

5.2.1 Context and Overview of the Cyberattack

In September 2023, MGM Resorts International was the victim of a cyberattack that caused significant operational disruptions across multiple properties. The company is considered one of the largest global corporations within the hospitality and entertainment

sector, managing an extensive network of casinos, particularly in Las Vegas. Such corporations exemplify highly digitalized business models that rely heavily on interconnected digital systems to manage core operations, which have consequently made strategic and highly vulnerable targets for cybercriminals (Schrader, 2025).

The cyberattack on MGM Resorts was a coordinated operation involving two criminal organizations, Scattered Spider and ALPHV, also known as BlackCat, and lasted approximately ten days, illustrating how human vulnerabilities can paralyze a highly digitalized corporate giant. (Schrader, 2025; Newman, 2023)

The initial phase consisted of infiltration and social engineering techniques. The initial breach was not technical but human. On September 8, 2023, after previously gathering information about MGM employees through platforms such as LinkedIn, the attackers used vishing (voice phishing) techniques to call the company's technical support service while impersonating employees, thereby obtaining login credentials. Once these credentials were acquired, the attackers expanded their control over the internal network by gaining administrative access to key identity management systems and cloud services used by the organization. This access allowed them to move laterally across the network to identify the most critical systems and attack them (Schrader, 2025).

At this stage, Scattered Spider collaborated with the group ALPHV, which operates under a ransomware-as-a-service model that provides malicious software designed to block or encrypt critical systems (Newman, 2023). Approximately 100 ESXi hypervisors supporting essential operational systems, including gaming machines or reservation systems, were encrypted. As a result, thousands of virtual machines became inoperative, causing the immediate operational paralysis of several hotels and casinos operated by the corporation. In addition to encrypting systems, the attackers implemented a double-extortion strategy, threatening to publish confidential customer information that had been extracted if the ransom was not paid. However, MGM Resorts, following the recommendations of the FBI and cybersecurity agencies, decided not to pay the ransom, opting instead to progressively restore its systems and contain the intrusion. Subsequently, the company faced class-action lawsuits filed by customers alleging negligence in the protection of their personal data (Schrader, 2025).

The impact of the attack became publicly visible on September 10, 2023, when systems such as slot machines and digital room keys began to fail across multiple properties. These

disruptions generated a wave of criticism, significantly affecting the company's public reputation (Schrader, 2025; Naraine, 2023).

Beyond its technical impact, the incident also had significant financial consequences. MGM reported losses exceeding $100 million during the third quarter, in addition to $10 million related to technological consulting, legal advisory services, and system recovery processes. In response to the crisis, the company announced an additional $40 million in investment in infrastructure and cybersecurity improvements aimed at strengthening its technological resilience. Overall, the MGM case illustrates how a cyberattack can rapidly escalate into a corporate crisis with operational, economic, and reputational implications, especially in highly digitalized organizations where technological dependence can quickly translate into tangible disruptions in service delivery (Schrader, 2025; Newman, 2023).

5.2.2 Corporate Response and Crisis Communication Strategy

Due to the highly digitalized environment in which MGM Resorts International operates, the corporation was forced to implement a crisis communication plan following the cyberattack in early September 2023, to strategically manage the situation and minimize, as much as possible, the reputational impact. The corporate response and crisis management strategy evolved progressively in three different stages, transitioning from technical containment to a final narrative of resilience.

In the first days following the attack, the company adopted drastic technical containment measures, prioritizing the disruption of the attack even if this implied limiting informational transparency in its initial communication. This first phase began with the publication of the company's first official statement on September 12, 2023. In this statement, MGM reported the situation by stating that it had identified "a cybersecurity issue affecting certain of the Company's systems" and indicated that it was "taking steps to protect our systems and data, including shutting down certain systems." (MGM Resorts International, 2023b). This constitutes the central element of the statement, as it frames the operational shutdown as a deliberate security decision to protect customers, thereby reframing a technical vulnerability as a preventive action under corporate control. Likewise, the language used throughout the statement was vague and strategically ambiguous, avoiding references to complex terms such as ransomware, to contain reputational damage within a context of heightened uncertainty (MGM Resorts International, 2023b).

However, although the crisis communication strategy managed to contain public alarm, a clear discrepancy soon emerged between the corporate discourse and the operational reality. As a consequence of the deliberate shutdown of systems, the company lost access to corporate email, being forced to use non-official channels. From a crisis communication perspective, this aspect is particularly relevant, as the medium is the message, and it is not possible to project an image of full control of the situation without doing so through its institutional voice. This undermined its credibility with the press and generated an information vacuum that resulted in frustration among customers on social media (Goswami, 2023).

This discrepancy between corporate communication and operational reality was reflected in social media reactions but also became visible on-site, as illustrated in Figure 2.

Figure 2

Social media evidence of operational disruption and customer-facing service limitations at MGM Resorts during the cyberattack.

Source: Hooks, 2023.

At the same time, while public communication in this initial phase maintained a minimalistic and moderate tone, in its first statement, the company was more explicit towards stakeholders by stating that the investigation was being carried out with "assistance from leading external cybersecurity experts" (MGM Resorts International, 2023b). Through this statement, MGM seeks to shift the perception of chaos towards professional management, reinforcing its legitimacy through the externalization of the

technical response. However, its crisis communication strategy reveals a certain communicative duality, as while the public discourse seeks to demonstrate that the incident is under control, on September 13, the company had to admit before the SEC that the incident represented a material risk for the company, showing itself more vulnerable and transparent in its financial communications (Goswami, 2023). After the initial hermeticism, a shift in the communication strategy towards greater transparency can be observed, aimed at reducing the uncertainty that had affected its market value and, at the same time, restoring stakeholder trust.

One of the key elements that evidences this change in the narrative is the Form 8-K report issued on October 5. The corporation was required to file this document with the US Securities and Exchange Commission (SEC) due to the relevance of the incident. In it, MGM states that "The Company estimates a negative impact from the cybersecurity issue in September of approximately $100 million" (MGM Resorts International, 2023a*),* quantifying the real financial impact in order to reduce investor speculation, which is considered one of the main stakeholders. Likewise, it acknowledges having incurred "less than $10 million in one-time expenses … related to the cybersecurity issue" (MGM Resorts International, 2023a). The quantification of the impact allows transforming an open crisis into a bounded loss, facilitating its absorption by the market.

This transparency is not only directed towards investors, but also towards customers, who are the other relevant stakeholder group. The company moves from referring to a cybersecurity issue to explicitly recognizing the data breach, complying with its legal and ethical obligations (MGM Resorts International, 2023c). Through its statement, it explained in detail what type of information had been compromised. The following statement stands out: "At this time, the Company does not believe that customer passwords, bank account numbers or payment card information were obtained by the criminal actors." (MGM Resorts International, 2023d).

This statement reflects a contrast strategy aimed at protecting its most critical asset, namely, consumer financial trust. This strategy consists of presenting first a negative event, which is the current data breach situation, together with a worse scenario that did not occur, so that the negative news appears less severe when compared to the catastrophic scenario that MGM managed to avoid (MGM Resorts International, 2023d).

In addition to detailing the compromised information, the company also explains in another section of the statement the measures it is taking to counteract the negative impact of the incident, such as the establishment of a help line or the provision of free identity protection and credit monitoring services to affected customers, thereby incorporating elements of a reputational repair strategy. (MGM Resorts International, 2023d).

Finally, the last phase, consolidated on October 10, 2023, represents the official closure of the crisis narrative. At this stage, CEO Bill Hornbuckle pivots public attention towards the future projection of the company, restoring leadership and stakeholder trust. The CEO acts as a closer or figure of maximum authority who assumes full control of the corporate response and answers the interviewer's questions with a rhetoric of absolute normality. The decision to give an interview in a high-level financial media outlet such as CNBC signals a strategic orientation towards investors as a primary audience.

Following the question about the extent to which the crisis had been left behind, the CEO states:

> It is totally behind us. Look, it was a hell of a three-week period. I cannot say enough about how resilient we are. I've got to call out the MGM employees — they've been nothing but great through this entire process. But this is behind us. Hopefully it's a one-time incident — knock on something quickly — and we're all moving forward. It had a significant impact, as you saw in September. There will be some lingering impacts in the first part of October. But then the balance of the quarter, through Formula One in December, we think we're in great shape (CNBC, 2023).

From an analytical perspective, this corporate response fulfills several key functions. The repeated use of the phrase "is totally behind us" (CNBC, 2023) constructs a temporal closure and signals a transition towards operational normality. The emphasis on employee performance introduces a component of corporate humanization which, in addition to projecting external strength, reinforces internal cohesion. Likewise, Hornbuckle appears transparent regarding the damage suffered during September and early October, which makes his future outlook be accepted as a financial reality rather than merely a corporate aspiration. This is reinforced in the following statements, where he acknowledges that the situation was not ideal, using a euphemism that validates reality without resorting to alarmist language that could reactivate negative frames among stakeholders.

> Look, it's not ideal, obviously. But again, MGM, Las Vegas, our group has been nothing but resilient. You think about all the things we've been through over the last four or five years. This is unfortunately, one more incident. But it is behind us. We're looking forward. There is work to do going forward in terms of restructuring, rebuilding and rearchitecting where we were versus where we'd like to get to. But all that is already in play. We feel extremely safe and secure where we are today and are looking forward to a great quarter (CNBC, 2023).

In these statements, the CEO places the cyberattack within a broader historical context. This is a way of normalizing the situation by associating it with previous challenges, making it appear as just another incident to overcome. On the other hand, by using the word resilient, MGM seeks to change the perception of the company from a victim of a cyberattack to an organization that has emerged stronger from the situation, rebuilding its reputation. Similarly, the use of terms such as "restructuring" or "rearchitecting" redirects attention towards future-oriented structural improvements, projecting an image of organizational learning and adaptation. This validates the information from the 8-K report, where these significant measures with external experts were mentioned. The final assertion that the company feels "extremely safe and secure" acts as a final anchoring point, consolidating the narrative of restored trust and shifting the focus towards the future growth opportunities associated with high-impact events such as Formula 1 (CNBC, 2023).

Overall, this final phase represents a discursive closure of the crisis, managing to transform a destabilizing incident into a narrative of institutional strengthening and resilience, thereby recovering legitimacy among stakeholders.

5.2.3 Theoretical Interpretation and Reputational Implications

Based on the previous empirical and discursive analysis of the MGM Resort International´s crisis response, this section shifts the analytical lens toward a theoretical interpretation.

From the perspective of the Situational Crisis Communication Theory (SCCT), the cyberattack can initially be classified as a victim cluster, since the origin of the action comes from an external criminal actor. In theoretical terms, the reputational threat would be limited, as this categorization implies low levels of attribution of responsibility (Ulmer et al., 2018; Coombs, 2007).

However, this classification proves to be unstable in the context of contemporary cybercrises, and the case of MGM is an example of this. The statement made by the CEO on October 10, 2023, in which he publicly admits that the entry vector was human error, shifts the crisis to a preventable cluster. This shift significantly increases the reputational threat and leads the public to reinterpret the crisis as the result of organizational negligence (CNBC, 2023).

This phenomenon reflects a structural limitation of SCCT in contemporary digital environments. As Jørgensen (2018) points out, in a cyberattack, stakeholders tend to attribute a much higher internal responsibility than what the SCCT model predicts. This mismatch can be explained by the fact that, in a digital context, stakeholders consider that it is the company's duty to protect their confidential information and data, which transforms the nature of the event into a manifestation of internal failure. Consequently, the strategy of victimization is insufficient in this context.

This reinterpretation can be understood more deeply through the analysis of how stakeholders construct responsibility in crises. Specifically, this process can be examined through the Attribution Theory, which is the psychological basis of SCCT. In the case of MGM Resorts International, this process is articulated around three key dimensions.

First, the locus of causality is initially configured as external since the attack is attributable to criminal actors. However, the revelation that the intrusion occurred through social engineering techniques targeting internal staff produces a partial shift toward an internal locus, thus increasing the attribution of corporate responsibility (Jørgensen, 2018).

Second, controllability evaluates whether the organization could have avoided the incident through adequate management. In the case of MGM, although the attack was an external criminal act, the class-action lawsuits against the company claim that the organization had the control to protect the data but failed in its duty by not implementing sufficient measures, such as data encryption. Therefore, the exploitation of human vulnerabilities reinforces this perception of predictability and causes the attribution of blame to increase (Jørgensen, 2018).

Faced with this dynamic, the organization attempted to mitigate the attribution of negligence through a strategy based on demonstrating operational control. Actions such as the rapid containment of the incident, the shutdown of affected systems, and the

involvement of external experts were key elements in constructing a narrative aimed at projecting response and recovery capacity. In this way, MGM sought to limit the interpretation of the crisis as a structural failure and reinforce the perception of organizational competence.

Finally, the stability factor is analyzed through the crisis history in order to examine whether the cyberattack was an isolated case or a recurring trend. The existence of a relevant precedent, such as the 2020 data breach, introduces a perception of recurrence that may lead stakeholders to interpret the incident as part of a systemic pattern (Goswami, 2023). From the perspective of Attribution Theory, this repetition reduces tolerance and amplifies negative reactions, as it suggests that the organization has not corrected previous vulnerabilities.

The combination of these factors creates a scenario of high responsibility attribution. This attributional framework increases the intensity of negative emotional responses and favors the adoption of punitive behaviors by stakeholders, such as loss of trust or the initiation of legal actions, which, in the case of MGM, began to emerge from September 2023 (Schrader, 2025).

In this setting, MGM's response shows a progressive adjustment to increasing levels of attributed responsibility, shifting toward more accommodative strategies as reputational threat intensified.

Complementing the SCCT analysis, Image Repair Theory (IRT) provides a rhetorical lens to dissect MGM Resorts International´s discursive strategies for mitigating the perceived image threat posed by the cyberattack (Benoit, 1997). For IRT to apply, stakeholders must attribute responsibility to the organization for an offensive act, in this case, the operational shutdown, data exposure, and customer inconvenience, which met both conditions given the lawsuits alleging negligence in data protection.

MGM's response unfolded as a hybrid strategy across IRT's five strategy categories, prioritizing forward-looking repair over denial. This approach centered primarily on corrective action and reducing offensiveness as mechanisms to counteract significant reputational and financial threats (Naraine, 2023; Benoit, 1997).

In order to distance the corporate entity from direct blame, the company utilizes specific sub-categories. The CEO framed the intrusion as an "accident" via human error (vishing

attack on the IT help desk) to position the crisis as a fortuitous event (CNBC, 2023). Within this category, the corporation also invokes defeasibility by noting in the 8-K Report that “no company can ever eliminate the risk of a cyberattack” (MGM Resorts International, 2023a) thus portraying the event as partially beyond organizational control despite prior warnings from suppliers like Okta (Schrader, 2025; Benoit, 1997). However, the effectiveness of this defeasibility strategy is limited as the acknowledgement of human error, together with the warnings from external providers, implicitly reinforced internal responsibility attributions.

As attributions intensified, MGM Resorts International shifted to reducing offensiveness, the most discursively active phase (Benoit, 1997). Firstly, the company used bolstering mechanisms by emphasizing their positive traits. The CEO Hornbuckle repeatedly praised the resilience of MGM Employees, stating that they were “nothing but great” (CNBC, 2023). Additionally, the arrival of the Formula One race shortly after the cyber incident was used as a narrative anchor to shift public focus toward recovery and financial strength (Schrader, 2025). Furthermore, minimization tempered perceived harm by repeatedly clarifying what was not stolen to make the breach seem less severe than reported (MGM Resorts International, 2023a). Lastly, compensation was materialized through free credit monitoring and identity protection services for affected customers (MGM Resorts International, 2023c), tactics empirically linked to image restoration when victims deem them adequate (Benoit, 1997). These strategies contributed to partially containing reputational damage; nevertheless, their effectiveness remained conditional upon stakeholder evaluations of organizational accountability, which increasingly framed the incident as a failure of organizational competence.

Corrective action emerged as the cornerstone strategy, aligning with Benoit´s view of it as highly effective for promising resolution and prevention. MGM's execution was robust. MGM committed $40 million to IT infrastructure upgrades (Schrader, 2025), announced they were “rearchitecting” their IT systems to close the detected gaps (CNBC, 2023), and highlighted collaboration with cybersecurity experts and the FBI (MGM Resorts International, 2023a). This demonstrates a discursive transformation of a vulnerability into proactive competence. In addition, through that strategy, the company addressed stakeholder demands for non-recurrence. Therefore, corrective action proved the most credible way to repair MGM's reputation.

Finally, the corporation expressed regret for all the inconvenience caused, but it did not fully apologize or admit guilt (Benoit, 1997). Thus, mortification remains circumscribed, a strategic restraint likely shaped by legal considerations amid class-action suits. Rather than full admission, the company expressed regret for disruptions and validated financial impacts ($100 million losses), avoiding litigation risks while softening the offender's image (Schrader, 2025). This measured approach contrasts with more accommodative apologies in lower-stakes crises.

Taken together, the effectiveness of MGM´s image repair strategy was high in terms of financial viability, as evidenced by the quick restoration of services. However, the previous crisis history conditioned stakeholders´ attributions of internal responsibility, thereby constraining the persuasive capacity of its communicative responses.

Ultimately, regarding corporate reputation, MGM´s response illustrates the limits of reputational capital as a buffer mechanism. While the company initially benefited from a strong prior reputation, the existence of previous crises in 2020 reinforced perceptions of recurrence, thereby weakening its buffering capacity (Coombs, 2007; Goswami, 2023). As a result, reputational capital did not operate as a stable shield, but a contingent resource dependent on stakeholder attributions.

6. Comparative Discussion

The analysis of the Sony Pictures Entertainment (2014) and MGM Resorts International (2023) cases reveals significant variations in crisis communication strategies, reputational trajectories, and stakeholder attributions despite both corporations confronting corporate cyberattacks. This comparative discussion examines three analytical dimensions: the evolution of crisis communication strategies across temporal contexts, the impact of hyperconnectivity on stakeholder expectations, and the configuration of reputational implications within contemporary digital environments. The objective is to identify patterns, divergences, and factors that condition the effectiveness of communicative responses in corporate cyber crises.

6.1. Evolution of Crisis Communication Strategies

The nearly decade-long temporal gap between the Sony (2014) and MGM (2023) cases provides an analytical opportunity to examine how crisis communication strategies have evolved in response to changing digital environments and organizational learning processes in the context of corporate cyberattacks. This comparison suggests a shift from

reactive models, constrained by operational urgency, toward a more proactive approach integrated into reputational risk management.

In earlier models, responses were often delayed as organizations wanted to gather complete information before engaging with stakeholders. However, in contemporary digital environments characterized by immediacy and hyperconnectivity, such delays generate an information vacuum in which external actors rapidly shape the crisis narrative. Sony exemplified this pitfall. The organization maintained a passive silence during the first week following the attack, characterized by minimal public communication and a low-profile victimization strategy. This initial lack of communication generated an information vacuum that was rapidly filled by media speculation and the gradual leakage of compromising internal emails concerning Hollywood talent (DeSimone & Horton, 2017). Thus, their absence allowed external actors to control the narrative framing of the crisis, thereby intensifying reputational damage before Sony could articulate a coherent response (Steinberg et al., 2021).

In contrast, MGM Resorts International responded with greater operational agility, issuing its first official statement shortly after detecting the intrusion (MGM Resorts International, 2023b). In this sense, the evolution from Sony to MGM strategies demonstrates that time is no longer a "wait-and-see" factor, but a proactive tool defined as "stealing thunder," that is, getting ahead of the news to retain control over the crisis narrative (Jørgensen, 2018). This contrast also reveals one of the SCCT's central mechanisms: digital crises compress attribution windows, requiring immediate alignment of timing, responsibility signals, and stakeholder perceptions (Coombs, 2007).

This evolution becomes more evident in the management of narrative control. While Sony attempted to position itself within the victim cluster of SCCT by emphasizing the unprecedented sophistication of a state actor such as North Korea through scapegoating (Jørgensen, 2018), this strategy proved ineffective. Stakeholders ultimately reclassified the crisis as preventable due to evidence of basic security failures, such as weak password practices. In contrast, MGM adopted a defeasibility strategy within the framework of Image Repair Theory, acknowledging that the attack originated from a "human error" through a vishing attack on the help desk, while also recognizing that no organization can fully eliminate cyber risk (Benoit, 1997; MGM Resorts International, 2023a). This form of controlled transparency reflects what can be understood as a shift towards a provisional communication (Ulmer et al., 2018). Although acknowledging the human error increases

perceived internal controllability, it reduces uncertainty more effectively than technical denial, thereby facilitating stakeholder forgiveness in a context where corporations are increasingly perceived as responsible custodians of digital privacy. This shift illustrates how the contemporary digital paradigm has significantly raised stakeholder expectations regarding organizational accountability.

Furthermore, the comparative analysis reveals a transformation in the structural role of communication within crisis management. Sony's response demonstrates how communication remained largely subordinated to unfolding events. Its response was fragmented and reactive, with data leaks exposing internal cultural issues, leading to executive resignations and financial losses estimated at $171 million, without a coherent strategic integration (Jørgensen, 2018). This lack of integration contributed to a deeper and more prolonged reputational erosion. By contrast, MGM integrated communication from the outset as part of a broader risk management system. This integration is evident in the 8-K filing, where the company immediately quantified quarterly losses of approximately $100 million and anchored its recovery narrative in future-oriented milestones such as the Las Vegas Formula 1 event. This difference goes beyond operational execution and reflects a broader evolution toward understanding communication as a strategic function capable of shaping perceptions of economic viability from the early stages of crisis management.

Finally, the adaptation to stakeholder expectations illustrates a shift from a generic apology toward practical self-efficacy. Sony failed to provide employees and customers with instructive information on how to protect themselves following the data breach, resulting in class-action lawsuits (DeSimone & Horton, 2017). In contrast, MGM prioritized the provision of instructive information and tangible corrective measures, including dedicated call centers and free credit monitoring services. This transformation demonstrates that, while mortification strategies—centered on sincere apologies—were traditionally central to image repair (Benoit, 1997), they are no longer sufficient in contemporary cyber crises. Today's stakeholder can be understood as a "political consumer" who demands concrete solutions in response to the psychological stress associated with identity theft. In this context, the evolution of crisis communication strategies also supports contemporary critiques of SCCT, according to which pure victimization is no longer an effective strategy (Jørgensen, 2018). Instead, in the current

digital paradigm, “doing”, through corrective action, has become significantly more credible than merely “saying” through symbolic apologies.

In sum, these elements demonstrate a transformation in crisis communication strategies within the contemporary digital environment. The comparison between Sony and MGM shows how corporations have moved toward integrating crisis communication as a dynamic process in which timing, narrative framing, responsibility attribution, and corrective actions operate in an interdependent manner. In this new paradigm, the effectiveness of communication depends not only on its content but also on how and when it is delivered, its alignment with stakeholder expectations, and its ability to project control and resilience even in conditions of high uncertainty.

6.2. Impact of Hyperconnectivity and Stakeholder Expectations

In the contemporary digital paradigm, hyperconnectivity can be understood as an independent structural condition that, in addition to influencing the speed of crises, has redefined the way stakeholders evaluate and interpret these incidents. The interconnection of systems and the constant circulation of real-time information have transformed cybersecurity crises into complex social and reputational events. This new reality is defined by an infrastructure of “tightly coupled” systems in which any local disruption generates a global domino effect, turning stakeholders into direct subjects of systemic and invisible risks (Lagadec, 2009). Thus, the organizational relationship has been transformed, as publics no longer perceive corporations as mere service providers but instead demand that they assume a role as mandatory custodians of digital privacy, prioritizing systemic resilience over retrospective image repair.

In a real-time communication environment, the diffusion of crisis-related news is almost instantaneous, reaching audiences within minutes after the confirmation of the event. This structural reality generates a context of constant uncertainty, while also eliminating the traditional margin of maneuver for organizations, creating continuous pressure to communicate rapidly. In this way, the so-called “information vacuum” emerges as an interpretative space where stakeholders actively construct meaning based on incomplete signals, external narratives, or leaked information. Therefore, if an organization fails to intervene quickly, the space may be quickly occupied by external actors, shaping the perceptions and expectations of those affected (Ulmer et al., 2018). The cases analyzed reflect this dynamic, showing that if the corporation occupies this space at an early stage, the consolidation of negative frames can be avoided.

Moreover, hyperconnectivity has transformed stakeholder expectations, expanding the so-called expectation gap (Coombs, 2007), understood as the discrepancy between perceived ethical standards and the actual performance of the organization. Stakeholders are no longer satisfied with formal apologies, but instead demand "significant choice" (Ulmer et al., 2018). This entails access to instructive information that enables autonomous self-protective actions, such as changing passwords or monitoring credit activity. This evolution reinforces the perception that positions corporations as ethical guarantors of privacy, where failure to meet these expectations is interpreted as a violation of the duty of care (Benoit, 1997).

From the perspective of SCCT, this environment challenges traditional crisis categorizations (Coombs, 2007). Although cyberattacks are theoretically positioned within the victim cluster, stakeholders in hyperconnected environments tend to attribute high internal responsibility when they perceive deficiencies in reasonable care or technical competence, especially if the recurrence of incidents suggests systemic failures (Jørgensen, 2018). Sony was reclassified as negligent due to weaknesses in encryption practices, whereas MGM acknowledged "human error" and facilitated stakeholder forgiveness through technical transparency.

Finally, hyperconnectivity entails a profound decentralization of narrative control, whereby corporations lose their monopoly over the construction of their own image. In this context, stakeholders and other digital actors act as arbiters of the collective framing of the crisis (Ulmer et al., 2018). As a result, reputational capital, although it continues to function as a buffer, is rapidly depleted if the crisis reveals recurring vulnerabilities. Overall, the comparison between Sony and MGM reveals that the ability to respond to dynamic stakeholder expectations and to reduce uncertainty in interdependent systems constitutes a central element in the construction of organizational legitimacy in the contemporary digital environment.

6.3. Reputational Implications in the Contemporary Digital Context

The comparative analysis of the cases of Sony Pictures Entertainment (2014) and MGM Resorts International (2023) reveals a structural transformation in the configuration of corporate reputation in digital environments. In this context, reputation shifts from being considered a static and retrospective asset to being understood as a dynamic asset of operational resilience and transactional risk that is negotiated in real time through processes of collective sense-making between the organization and its stakeholders.

In the digital era, communication has ceased to be unidirectional and has become dynamic and participatory, as any user simultaneously acts as both a producer and distributor of information. As a result, reputation becomes a highly vulnerable asset that can be destroyed in a short period of time due to the rapid dissemination of information and virality. Therefore, stakeholder judgments are formed as the event unfolds, which highlights the need to build a strong reputation throughout the entire crisis communication process (Kuswati et al., 2025). In this context, initial communication decisions acquire a path-dependent nature, as once a negative interpretative frame is consolidated, it becomes difficult for the corporation to reposition itself strategically (Coombs, 2007).

In this contemporary digital context, reputation is no longer understood solely as a matter of image or prestige but is also understood as a quantifiable signal of transactional risk. When stakeholders perceive that a company is "too risky" to operate with, they make concrete decisions such as canceling contracts, withdrawing investments, or initiating legal actions (Kamiya et al., 2021). This can be observed in both the Sony and MGM cases, where reputational damage extended beyond the symbolic impact. In particular, the MGM case shows that in digitally transformed businesses, system failures translate directly into immediate financial consequences.

The comparative analysis shows that reputational damage acquires an economic dimension that goes beyond the direct costs of the incident. Through implicit valuation mechanisms such as shadow pricing, stakeholders assign a monetary value to intangible assets such as trust and credibility (Perera et al., 2022). While in the Sony case, reputational impact manifested more diffusely through the leakage of sensitive information and the loss of symbolic capital, in the MGM case, it translated more directly into measurable financial indicators, including operational losses and warnings regarding its credit risk profile. This difference demonstrates that, in highly digitalized environments, reputational damage evolves from an image-related crisis into a structural challenge linked to solvency and cost of capital.

This transformation also reflects the growing integration of reputation into corporate risk. In this sense, the perception of technical negligence, such as weak passwords or insufficient encryption, automatically shifts the crisis from the victim cluster to the preventable cluster (Coombs, 2007). In these cases, reputational damage becomes irreversible without a concrete demonstration of operational resilience. Therefore, contemporary reputation depends less on being invulnerable and more on the capacity for

cyber-resilience, understood as the ability to contain systemic damage and restore critical functions rapidly (Toma et al., 2023).

Likewise, the traditional "reputational buffer" becomes contingent. When incidents suggest stability (structural recurrence), this prior capital is rapidly depleted, transforming technical failures into moral judgments about organizational integrity (Coombs, 2007). Contemporary reputation is ultimately validated by user self-efficacy: the organization's ability to empower affected stakeholders with concrete tools for post-crisis self-protection (Ulmer et al., 2018).

In sum, digital reputation measures operational legitimacy rather than symbolic prestige, becoming integrated as a structural variable within total corporate risk, where each crisis constantly reconfigures the organization's strategic position (Kuswati et al., 2025).

7. Conclusions

This final chapter synthesizes the main findings derived from the theoretical and empirical analysis developed throughout the study. Based on the comparative examination of the cases of Sony Pictures Entertainment (2014) and MGM Resorts International (2023), structural patterns are identified in the communicative management of cyber crises and their impact on the configuration of reputational trajectories.

7.1. Answer to the Research Question

The research has directly addressed the central research question: How do the crisis communication strategies adopted during corporate cyberattacks influence the configuration of reputational damage and subsequent reputational recovery processes?

The results demonstrate that crisis communication constitutes a structural component within reputational risk management rather than merely a reactive response. It operates through three interdependent mechanisms, namely the narrative of the event, the mediation of responsibility attribution, and strategic adaptation to the current digital environment. These mechanisms collectively determine the magnitude of reputational damage and its possibilities for reversibility.

First, the primary mechanism explaining the formation of reputational damage is the attribution of responsibility. The findings indicate that reputational impact arises from how stakeholders interpret its causes based on the dimensions proposed by SCCT (locus of causality, controllability, and stability), rather than from the cyberattack itself. From

this perspective, cyberattacks are situated in an attributional grey area, since although they are technically external, if negligence in prevention or security management is perceived, interpretation shifts toward internal responsibility. In the analyzed cases, this phenomenon is evident: while Sony was progressively perceived as negligent due to the exposure of fundamental vulnerabilities, MGM experienced a partial shift toward internal attribution following the acknowledgment of human error. As a result, negative emotions intensify, and prior reputational capital weakens, confirming that attribution constitutes the central mediating link between the event and its reputational effects. Therefore, these results allow us to conclude that responsibility attribution directly conditions reputational trajectories.

Second, the construction of narrative framing constitutes a fundamental mechanism for shaping stakeholder interpretation. In contexts of high uncertainty, communication not only transmits information but also structures the meaning of the event. When the corporation articulated a coherent narrative aligned with empirical evidence and accompanied by specific actions, interpretative ambiguity is reduced, and the consolidation of negative frames is avoided. Conversely, reactive, or inconsistent responses transfer narrative control to external actors, particularly in digital contexts, which increases reputational damage. The Sony case shows how a contradictory and delayed framing facilitated the consolidation of negative interpretations, whereas MGM, through a progressive narrative focused on corrective action and resilience, was able to partially mitigate its impact. Therefore, it can be concluded that narrative framing decisively influences the evolution of reputational damage and recovery by structuring the interpretative process in contexts of uncertainty.

Finally, the differentiated digital contexts between Sony (2014) and MGM (2023) critically condition the effectiveness of communication strategies. The evolution between 2014 and 2023 reflects how hyperconnectivity has significantly compressed response times. Sony had weeks to react, whereas MGM had to act within less than 24 hours to prevent platforms such as X, TikTok, and Reddit from shaping the narrative. In parallel, stakeholder expectations also changed. Sony could rely on general statements, whereas MGM needed to provide more concrete and quantifiable information, such as specific technical and corrective measures implemented. Likewise, narrative control has become fragmented, shifting from an environment dominated by traditional media to a decentralized ecosystem in which multiple digital actors, such as forums, actively

participate in constructing the meaning of the crisis. Consequently, it can be concluded that contemporary digital environments not only condition but can significantly amplify or mitigate reputational impact depending on the organization's adaptive capacity. This is evidenced by the comparatively faster recovery trajectory observed in MGM. Thus, the digital context emerges as a determining variable that redefines the parameters of communicative effectiveness.

In synthesis, crisis communication does not merely respond to the effects of a cyberattack, but actively shapes its reputational impact by influencing stakeholders' processes of interpretation, evaluation, and response. Therefore, its effectiveness depends on the organization's capacity to align its communicative strategies with the demands of the contemporary digital environment, characterized by immediacy, uncertainty, and decentralized narrative control, ultimately determining whether a crisis results in prolonged reputational erosion or a manageable recovery process.

7.2. Theoretical and Practical Implications

From a theoretical perspective, the findings of this study substantiate the necessity to reconsider the application of established crisis communication models in relation to corporate cyber crises. The analysis revealed that the attribution processes of cyber crises do not fully align with traditional theoretical assumptions, as stakeholders increasingly interpret organizations as responsible for safeguarding digital infrastructures, even when crises were caused by external factors. This challenges the conventional categorizations and suggests that attribution processes in cyber crises are structurally intensified.

Furthermore, the study also shows that traditional crisis communication models do not fully comply with the realities of modern digital environments, as communicational effectiveness is strongly conditioned by temporal factors, where immediacy and early intervention become central to maintain narrative control. This highlights the necessity of incorporating a temporal dimension into the existing theoretical frameworks analyzed, which are SCCT and IRT, shifting towards a more dynamic and anticipatory approach.

In addition, reputation emerges as a dynamic and contingent resource continuously negotiated through real-time interactions between the corporation and its stakeholders. This reconfiguration underscores its integration within broader structures of operational resilience and management.

From a practical point of view, the research revealed a necessity to develop communicational capabilities specifically adapted to cyber crisis environments. Corporations must be prepared to respond rapidly, providing clear, concrete, and actionable information from the early stages of the crisis. At the same time, it is essential to align communicational capabilities with stakeholder expectations in order to reduce uncertainty and avoid the consolidation of negative interpretive frames.

Ultimately, effective crisis communication in contemporary digital environments depends on an organization's ability to demonstrate control, transparency, and adaptive learning. These elements are critical to mitigate reputational damage, as well as to facilitate a sustainable recovery process.

7.3 Limitations and Future Research

Despite the analytical value of the selected cases, certain limitations should be acknowledged.

Firstly, the present research is based on a qualitative comparative case study design involving two cases, which restricts the generalizability of the findings in relation to the broader domain of corporate cyber crises. The research objective is not based on any statistical generalization; rather, it is focused on the development of an in-depth analytical understanding of the communicational dynamics surrounding corporate cyber crises.

Secondly, the present research is based on the analysis of publicly available sources in relation to the selected cases. The sources are particularly relevant for examining the public dimension of corporate crisis communication and the overall narratives in relation to the crises. However, they may not fully capture the internal decision-making aspects that shaped the organizational responses to crises.

Thirdly, the analysis primarily focuses on formal corporate communication, which may overlook informal or decentralized narrative dynamics emerging in social media or other platforms of the digital environments.

Finally, the analysis of reputational implications is necessarily based on certain qualitative aspects since the concept of corporate reputation is a complex and socially constructed concept shaped by stakeholder perceptions and public interpretations.

Building on these limitations, future research should address three priority directions aligned with the study´s theoretical and methodological constraints.

In the first place, experimental studies testing the recalibration of SCCT for cyber crises would be particularly valuable to examine whether stakeholders systematically attribute higher levels of internal responsibility than those predicted by traditional crisis categorizations.

Furthermore, the quantification of stealing thunder effects requires the systematic examination of temporal dynamics through real-time social media monitoring across platforms such as TikTok or X. Likewise, comparative analysis between delayed and immediate (<24 hours) responses would enable a more in-depth assessment of how response timing shapes reputational trajectories.

Taken together, these research directions extend the findings of the study and contribute to the adaptation of crisis communication in contemporary digital environments.

Bibliography:

Barnett, M. L., Jermier, J. M., & Lafferty, B. A. (2006). Corporate reputation: The definitional landscape. *Corporate Reputation Review,* 9(1), 26–38. https://doi.org/10.1057/palgrave.crr.1550012

Beaumont-Thomas, B. (2014, December 10). Angelina Jolie called "minimally talented spoiled brat" in hacked Sony emails. *The Guardian.* https://www.theguardian.com/film/2014/dec/10/sony-hack-eamils-angelina-jolie-scott-rudin-amy-pascal-david-fincher

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177–186. https://doi.org/10.1016/S0363-8111(97)90023-0

Benoit, W. L. (2013). Image repair theory and corporate reputation. In C. E. Carroll (Ed.), *The handbook of communication and corporate reputation* (pp. 213–221). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118335529.ch19

CNBC. (2023, October 10). *MGM Resorts CEO Bill Hornbuckle: Cyberattack is behind us, and we're looking forward* [Video]. https://www.cnbc.com/video/2023/10/10/mgm-resorts-ceo-bill-hornbuckle-cyberattack-is-behind-us-and-were-looking-forward.html

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., & Holladay, S. J. (2005). An exploratory study of stakeholder emotions: Affect and crises. In N. M. Ashkanasy, W. J. Zerbe, & C. E. J. Härtel (Eds.), *Research on emotion in organizations: The effect of affect in organizational settings* (Vol. 1, pp. 271–288). Elsevier. https://doi.org/10.1016/S1746-9791(05)01111-9

DeSimone, A., & Horton, N. (2017). *Sony's nightmare before Christmas: The 2014 North Korean cyberattack on Sony and lessons for U.S. government actions in cyberspace* (National Security Analysis Department Report NSAD-R-17-045). Johns Hopkins University Applied Physics Laboratory.

https://www.jhuapl.edu/sites/default/files/2022-12/SonyNightmareBeforeChristmas.pdf

Federal Bureau of Investigation. (2014, December 19). *Update on Sony investigation.* https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Fotis, F. (2024). Economic impact of cyberattacks and effective cyber risk management strategies: A light literature review and case study analysis. *Procedia Computer Science*, *251*, 471–478. https://doi.org/10.1016/j.procs.2024.11.135

Goswami, R. (2023, September 14*).* MGM Resorts says cyberattack could have material effect on company. *CNBC*. https://www.cnbc.com/2023/09/13/mgm-resorts-cyberattack-and-outage-stretches-into-third-day.html

Hooks, R. [@rachaelhooks]. (2023, September 14). Ridiculous check in queues and casinos down… this is The Aria but seeing the same at many MGM resorts in Vegas. The MGM hack is causing chaos #mgm #mgmhack #mgmhacked #lasvegas [Post on X]. https://x.com/rachaelhooks/status/1702440630398460066

IBM Security. (2025). *Cost of a data breach report 2025*. IBM Corporation. https://www.ibm.com/reports/data-breach

Jørgensen, E. U. (2018). *The stakeholder attributions of corporate crisis responsibility following a cyberattack* [Copenhagen Business School]. https://research-api.cbs.dk/ws/portalfiles/portal/59754091/427671_Elisabeth_Jorgensen_digital.pdf

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *141*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kuswati, Y., Kusmayadi, D., & Pratomo, H. W. (2025). Maintaining public trust and reputation in the digital age. *IJESS International Journal of Education and Social Science, 6*(1), 133–138. https://doi.org/10.56371/ijess.v6i1.432

Lagadec, P. (2009). A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice. *Review of Policy Research, 26*(4), 473–486. https://doi.org/10.1111/j.1541-1338.2009.00396.x

Laughland, O., & Rushe, D. (2014, December 19). Sony cyber-attack linked to North Korean government hackers, FBI says. *The Guardian.* https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official

MGM Resorts International. (2023a, October 5). *Form 8-K*. U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

MGM Resorts International. (2023b, September 12). MGM Resorts International statement on cybersecurity issue. *PR Newswire.* https://investors.mgmresorts.com/2023-09-12-MGM-RESORTS-INTERNATIONAL-STATEMENT-ON-CYBERSECURITY-ISSUE

MGM Resorts International. (2023c, October 5). MGM Resorts update on recent cybersecurity issue. *PR Newswire.* https://www.prnewswire.com/news-releases/mgm-resorts-update-on-recent-cybersecurity-issue-301949001.html

MGM Resorts International. (2023d, October 5). *Notice of data breach.* https://www.mgmresorts.com/en/notice-of-data-breach.html

Naraine, R. (2023, October 6). MGM Resorts says ransomware hack cost $110 million. *SecurityWeek.* https://www.securityweek.com/mgm-resorts-says-ransomware-hack-cost-110-million/

National Institute of Standards and Technology. (2013). *Glossary of key information security terms* (NIST Interagency/Internal Report (NISTIR) 7298 Rev. 2). https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Newman, L. H. (2023, September 16). Massive MGM and Caesars hacks epitomize a vicious ransomware cycle. *Wired*. https://www.wired.com/story/mgm-ceasars-hack-ransomware/

Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors affecting reputational damage to organisations due to cyberattacks. *Informatics, 9*(1), Article 28. https://doi.org/10.3390/informatics9010028

Rushe, D., & Laughland, O. (2014, December 18). Sony Pictures scraps release of The Interview after theaters pull out. *The Guardian*. https://www.theguardian.com/film/2014/dec/18/fbi-north-korea-sony-pictures-hack-the-interview

Schrader, D. (2025, August 18). An overview of the MGM cyberattack. *Netwrix*. https://netwrix.com/en/resources/blog/mgm-cyber-attack/

Sony Pictures Entertainment. (2014a, December 23). *Sony Pictures Entertainment announces limited theatrical release of The Interview on Christmas Day* [Press release]. https://www.sonypictures.com/corp/press_releases/2014/12_14/122314_theinterviewtheatrical.html

Sony Pictures Entertainment. (2014b, December 24). *Sony Pictures to distribute The Interview online beginning Christmas Eve through Google Play, YouTube Movies, Microsoft's Xbox Video and dedicated website* [Press release]. https://www.sonypictures.com/corp/press_releases/2014/12_14/122414_theinterview.html

Steinberg, S., Stepan, A., & Neary, K. (2021). *The hacking of Sony Pictures: A Columbia University case study.* Columbia University, School of International and Public Affairs. https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

Toma, T., Décary-Hétu, D., & Dupont, B. (2023). The benefits of a cyber-resilience posture on negative public reaction following data theft. *Journal of Criminology, 56*(4), 470–493. https://doi.org/10.1177/26338076231161898

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2018). *Effective crisis communication: Moving from crisis to opportunity* (4th ed.). SAGE Publications.

Valackienė, A. (2010). Efficient corporate communication: Decisions in crisis management. *Inzinerine Ekonomika–Engineering Economics*, *21*(1), 99–110. https://doi.org/10.5755/j01.ee.66.1.11657

Verizon. (2025). *2025 data breach investigations report.* https://www.verizon.com/business/resources/reports/dbir/

World Economic Forum. (2025). *Global cybersecurity outlook 2025.* https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). SAGE Publications.