Capstone

Crisis Simulations of Deepfake CEO Fraud Videos in the Tech Sector: Measuring Investor Trust and the Effectiveness of Proactive vs. Reactive Communication Strategies

By: Avantika Vital

School of Professional Studies, New York University

Instructor: Prof. Stephanie Mattera
Advisor: Prof. Catalina Mejia Arenas

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Public Relations and Corporate Communication

Fall 2025

Disclaimer

This document is not for NYU-affiliated publication or distribution.

Please note that this study has not been reviewed or approved by an Institutional Review Board.
The Capstone is for educational purposes only and is not intended for publication or distribution.
If published, it must be presented as an unaffiliated project, not associated with NYU

Acknowledgment

I would like to express my heartfelt gratitude to **Prof. Mattera** and **Prof. Arenas** for their invaluable guidance, support, and encouragement throughout the development of this capstone project. Their mentorship and thoughtful feedback have been instrumental in shaping both my research and professional growth.

Above all, I dedicate this work to **my mother**, whose unwavering love, strength, and belief in me have been my greatest source of inspiration and perseverance.

Abstract

This study investigates how corporate communication strategies influence investor trust during deepfake-related crises in the technology sector. Using a mixed-methods design, the research integrates qualitative content analysis of real-world synthetic-media incidents (2018–2024) with a quantitative, scenario-based experiment. The content analysis identifies key response traits: timing, tone, and transparency - used by organizations confronting deepfake events. The experimental survey (N = 30) randomly assigned participants to proactive or reactive response conditions and measured perceived trust, transparency, emotional reaction, and investment intention through Likert-scale items. Results from independent-samples *t*-tests and Cronbach's α analyses revealed that proactive communication consistently produced higher mean scores across all constructs, with medium-to-large effect sizes, though not all differences reached statistical significance. These findings support Situational Crisis Communication Theory by demonstrating that timely, transparent responses enhance credibility and stakeholder confidence. The study contributes to investor-relations scholarship by offering empirical insight into managing synthetic-media crises and underscores the growing need for proactive digital-reputation strategies in corporate communication.

Content

Chapter 1

Introduction

1.1 Background

Within the digital-first financial environment of today, effective executive communication is crucial in shaping investor attitudes and market actions, particularly within the tech sector. Studies indicate that CEO announcements, particularly those related to quarterly earnings reports, mergers, or regulatory updates, have a significant impact on stock prices (Jiang, Petroni, & Wang, 2010).

The authority of these high-pressure communications is being eroded by the emergence of deepfake AI videos that can misrepresent individuals issuing declarations they never actually made. Although deepfakes have garnered considerable scholarly and media attention in the fields of politics, journalism, and entertainment (Chesney & Citron, 2019; Vaccari & Chadwick, 2020), their impact on business leadership, investor confidence, and crisis communication remains less understood. This opinion is considered to be very harmful and dangerous, particularly due to the increasing use of synthetic media technologies and the very serious consequences of a doctored CEO video, which seems to be announcing the financial success or regulatory approvals of the company.

One example of this happened in 2023 when a company in Hong Kong was tricked by a deepfake video call of its CEO and thus lost more than $25 million (Regan, 2024). These incidents draw attention to financial and reputational risks that business organizations face with regard to the use of fabricated media. In such extremely dangerous situations, the response of the business in terms of speed, clarity, and transparency becomes very crucial in retaining stakeholder trust and preventing market instability (Coombs, 2014).

There is still no empirical consensus regarding which approach is more effective in the long term: an instant and active denial or a late and reactive one, in restoring investor confidence after a deepfake crisis. Current frameworks of crisis communication, including the Situational Crisis

Communication Theory (SCCT), emphasize the importance of timely and coherent messaging (Coombs, 2007); however, they are not typically applied to situations involving synthetic media. As West (2019) notes, the automation of corporate functions creates new vectors for reputational risk, particularly when trust hinges on the perceived presence and voice of leadership.

With the growing complexity of AI-based disinformation, it is crucial to understand how investors perceive and respond to various corporate response measures following deepfake events. This research endeavors to do this by bridging real-world deepfake case analyses and investor perception data with the growing body of literature on crisis communication, digital misinformation, and investor relations in the era of synthetic media.

1.2 Problem Statement

In the technology sector of the U.S., public announcements from CEOs regarding quarterly profits are considered very important in determining investors' actions and consequently stock prices. The emergence of AI-generated deepfake videos is one of the serious threats to this communication channel. These very lifelike videos can mislead viewers into believing a CEO is stating overblown revenues, mergers, or approvals; such statements, if taken at face value, could lead to stock price changes that are opposite to the actual situation before the reality is disclosed. Though the financial and reputational risks of deepfakes are obvious, very few firms have tried to find out what their response should be if such a deepfake is aimed at the CEO. Currently, there is no evidence-based advice as to whether a prompt (proactive) denial is better at preserving investor trust than an after-the-fact (reactive) response post fact-checking or internal review. Consequently, investor relations and corporate communications departments are not equipped to handle a major, urgent crisis.

The company's inability to act swiftly and strategically in accordance with the situation will result in a loss of trust from investors, share price fluctuations, and gradual damage to the firm's reputation as the worst-case scenario. The current research takes advantage of this gap by setting up the most challenging and risky crisis scenario, a deepfake-induced false CEO earnings announcement, and studying the stockholder reactions to different communication tactics.

1.3 Significance of the study

With the continuous improvement and wider availability of deepfakes and other synthetic media technologies, the risk they bring to business communication, investor trust, and even market stability is a matter that needs to be considered very seriously. Though there have been studies that looked into the political, journalistic, and social dimensions of deepfakes (Chesney & Citron, 2019; Vaccari & Chadwick, 2020), the question of influence in investor perception and behavior in the corporate world, especially in the tech sector, which is constantly in the limelight and under scrutiny, has not received much attention. This paper not only highlights the need for more research in this direction but also contributes to theoretical advancement by providing empirical evidence of the effects of different corporate response strategies to deepfake CEO videos on investor trust. By contrasting proactive versus reactive responses, this study sheds further light on how timing, tone, and transparency shape stakeholder attitudes during digitally mediated crises. The application of Situational Crisis Communication Theory (SCCT) to the new challenges arising from AI-generated disinformation represents a fresh use of an existing framework (Coombs, 2007).

The practical applications of this study are significant. For crisis response strategists, corporate communication officers, and investor relations teams, this research provides implementable guidance on designing response protocols for attacks from synthetic media. It can be used to inform

corporate playbooks, enhance preparedness training, and inform the creation of AI-focused crisis response frameworks. In addition, the research provides a launching pad for future inquiries into the changing interplay of artificial intelligence, trust, and communication strategy. As generative technologies blur the line between real and fake, understanding how people react to synthetic content becomes increasingly critical. These insights help ensure
corporate resilience, safeguard public market trust, and strengthen communication integrity in the age of digital media.

1.4 Purpose Statement

The research is intended to reveal to the public how AI-based deepfake videos have changed the perception of corporate credibility and crisis management, especially when misinformation directed at the CEO is the context. The majority of previous research has been directed toward the use of deepfakes in politics and media, whereas the impact of deepfakes on public companies, investor trust, and corporate communication strategies has almost completely been neglected by the academic world.

The study will involve a mixed-method approach, with content analysis of recent corporate deepfake incidents, along with a survey being conducted amongst the general public to measure levels of trust and legitimacy in such scenarios. The content analysis will consider media reports and company responses to known deepfake incidents between 2018 and 2024, including response time, tone, and level of transparency. The survey will capture individual perceptions
regarding how deepfakes could impact their investment decisions and their trust in leadership in a crisis.

By bridging real-world examples with perception data, this research aims to identify how companies can develop more effective, trust-preserving communication strategies in the face of synthetic media threats, filling a key gap in crisis communication and investor relations literature.

1.5 Hypothesis

If a tech company issues an immediate, proactive communication response to a deepfake video falsely depicting its CEO, **then** investors will be more likely to maintain trust in the company and its leadership, compared to when the company issues a delayed, reactive response. This expectation is supported by crisis communication theory, which emphasizes the importance of speed and transparency in preserving stakeholder confidence (Coombs, 2014; Vaccari & Chadwick, 2020).

1.6 Organization of the Study

This Capstone project is organized into five chapters, each building upon the previous to explore how deepfake CEO videos impact investor trust and the effectiveness of crisis communication strategies in the tech sector.

Chapter 1: Introduction

This chapter presents the research problem, provides the necessary background information, describes the objectives and significance of the study, formulates the research questions and hypotheses, and explains the key terms used throughout the investigation.

Chapter 2: Literature Review

The research on deepfake technology, investor behavior, crisis communication theories (such as Situational Crisis Communication Theory), and synthetic media in business environments is

reviewed in this chapter. It places the research in the context of relevant academic frameworks and points out shortcomings in the existing literature.

Chapter 3: Methodology

This chapter discusses the chosen mixed-methods approach and the research design, which consists of a quantitative survey and a content analysis of actual deepfake incidents. The participant selection process, data collection, and data analysis are all detailed in this chapter.

Chapter 4: Findings and Analysis

The content analysis and survey results are discussed in this chapter. It also explores the investor reactions to the communication strategies of the crisis, depending on their selection being proactive or reactive, and this leads to the identification of the existing trends, correlations, and insights in crisis communication practice.

Chapter 5: Discussion, Conclusions, and Recommendations

The last chapter of the capstone relates the findings to the research questions and theoretical underpinnings. Besides, it handles the implications of corporate communication and the investor relations team's practice, recognizes the limitations of the study, and thus presents future research avenues.

Chapter 2

Abbreviated Literature Review

2.1 Theoretical Frameworks: Anchoring Deepfake Crises in PR Theory

Situational Crisis Communication Theory (SCCT), developed by W. Timothy Coombs, has long served as a foundational framework for guiding how organizations should respond to different types of crises based on perceived responsibility and reputational threat. SCCT classifies crises such as victim (e.g., natural disasters, product tampering), accidental (e.g., equipment failures), and preventable (e.g., organizational negligence), and prescribes response strategies, ranging from denial and justification to apology and compensation, based on the level of attributed blame (Coombs, 2007). However, the rise of synthetic media, particularly deepfake videos targeting corporate leaders, reveals key limitations in SCCT's applicability. Deepfake incidents, while originating from external sources, often blur the lines between Coombs' categories. On the surface, they resemble victim crises, as the organization is under attack from a malicious external actor. However, attributional ambiguity is high, and viewers may believe the CEO genuinely made the statement, especially in the absence of immediate rebuttal, making them resemble accidental crises. Further, when such attacks exploit known security vulnerabilities or internal lapses in mediaverification, stakeholders may frame them as preventable, which in turn increases their reputational risk.

This tripartite nature of deepfake incidents creates what Schwartz (2025) describes as an "attributional trap." A company following the SCCT guidance and going on the offense with the denial of the deepfake by means of "attacking the accuser" or scapegoating (which are typical for rumor-type crises) will certainly look defensive at the very least, or even worse, like it has something to hide. On the other hand, in case the company goes for the overcorrection, implicitly

admits guilt or wrongdoings, and shows excessive remorse, it is likely to get itself into the trap of custodial and reputational liabilities, particularly if stakeholders view the incident as a result of poor cybersecurity measures or lack of leadership control. Recognizing this theoretical gap, Vecchietti et al. (2025) propose a Modified SCCT Matrix tailored to synthetic media crises.

2.2 Key Theme 1: Organizational Authenticity Theory: Building Trust Reserves

Deepfakes are big-time corporate threats to public credibility, as they corrode the four founding dimensions of perceived authenticity underpinning leadership communication: consistency, transparency, morality, and correctness. As stated by Vecchietti et al. (2025), these dimensions constitute the foundational core of stakeholder trust, especially in high-stakes sectors such as technology, where executive communication becomes almost a brand signal. To start, egregious acts of inconsistency occur for synthetic content when behaviors or messages starkly contradict a CEO's public persona or previous statements, culminating with an alarming degree of cognitive dissonance on the side of stakeholders. On the other hand, second are the issues concerning transparency undermined by the inability to verify the AI-generated origin of videos; in essence, even observers trained to note discrepancies have difficulties making such differentiations, particularly when such content travels speedily on unmoderated digital spaces. Third, the moralistic dimension proceeds from producing deepfakes for illegal activities, which allow the simulation of unethical or controversial conduct of interest. These levels of questionable conduct could be, for instance, insider trading, making disparaging remarks about discrimination, or political endorsements that will trigger deep outrage and damage reputation. Lastly, correctness is compromised when deepfakes include fabricated technical claims or falsified financial disclosures, eroding confidence in corporate leadership’s competence and integrity.

Schwartz (2025) portrays this as unlike brand equity management: credibility takes a long time to be built through sustained visible investments; in times of doubt, these are the investments acting like repurposed credibility. Adobe currently issues blockchain-backed press releases and CEO announcements, embedding cryptographic markers that allow any third party to check the origin of content in real time. Other companies have put watermarking to good use by embedding encrypted hash values in visual communications so that any instance of tampering can be immediately red-flagged. New reporting indicates a quarter live streaming proof-of-humanity program, whereby high-level tech folks engage in open-ended interactions with stakeholders to reassert relevancy, legitimacy, and control over the communication channels. Crisis communication can be understood in another way if we think of it as a form of communication that signals credibility ahead of time rather than as a forceful method to control damages after a public relations disaster. In a media atmosphere that is getting more and more dirty due to fake news, organizations that openly invest in such things as transparency, traceability, and communication by human beings are then able to go through deepfake-related crises and keep their investors' trust more easily.

2.3 Key Theme 2 : Media Richness & Uncertainty Reduction: Channel Dynamics

The deepfake technology inherently takes advantage of the psychological misconceptions that the **Media Richness Theory** involves by using excellent-quality video and audio to create the sense of realism of the digital impersonation. The theory of media richness, stated by Daft and Lengel, posits that communication through richer media (face-to-face, video, etc.) is more effective for handling ambiguous situations because they can provide nonverbal signs, instant feedback, and overall emotional tone. Nevertheless, in the case of deepfake disinformation, this line of reasoning that has been scientifically developed turns into a weakness. As Wagner and Chen (2025) argue, deepfakes weaponize the human bias toward equating media richness with truthfulness. A convincingly forged CEO video, complete with realistic facial expressions and voice patterns, can be more persuasive

than a genuine text-based denial, even when the latter is factually accurate. This creates what they term a **"paradox of verification"**: stakeholders inherently trust the deceptive, high-richness content while remaining skeptical of lower-richness channels, such as press releases or tweets, used for rebuttals. Organizations, therefore, face a serious communicative disadvantage when correcting synthetic misinformation.

Organizational Authenticity Theory (OAT) gains new relevance in delayed-response scenarios. A longitudinal study tracking 20 deepfake incidents found that companies taking >4 hours to respond suffered a 34% decline in perceived leadership transparency (Harvard Business Review [HBR], 2024). This aligns with OAT's emphasis on consistency as a trust safeguard.

The paradox is made even worse by **Uncertainty Reduction Theory (URT)**, which states that people try to get rid of uncertainty very quickly. In stock markets, this is seen in the behaviour of "herd skepticism," where investors, being presented with a deepfake that is unverified but very vivid, are likely to conclude that the worst has happened, thus deciding to sell their shares and protect their assets instead of waiting for proof. This behavioral pattern aligns with findings from Manhattan Strategies (2025), which documented that during synthetic crisis simulations, over 70% of retail investors reacted with immediate divestment before the company had issued a response.

In light of these challenges, experts recommend a **multi-channel verification strategy** that combines forensic AI analysis reports (traditionally low in media richness) with authenticated, high-richness rebuttals such as real-time CEO video responses containing digital watermarks or cryptographic signatures. The combination of credibility and channel fidelity is psychologically bridged with the help of this pairing. Altogether, these tactics show the consensus that has been developing and is now recognizing that the communication of a crisis in the age of deepfakes not only needs to be fast and clear but also requires the conscious management of the psychology of the channels and the understanding of the investors.

2.4 Key Theme 3: Deepfake Impacts: Reputational, Financial, and Regulatory Consequences

2.4.1 Reputational Damage: The Asymmetry Principle

Deepfake-induced crises unfold in a distinct and increasingly well-documented temporal arc that profoundly shapes their reputational impact. According to recent studies, deepfake incidents typically trigger a **three-phase model of reputational decay**, each with unique dynamics and implications for crisis response timing and resource allocation.

The first phase, **Contagion** (0–2 hours), begins immediately after the synthetic media is released or leaked. During this window, screenshots, screen recordings, and compressed versions of the deepfake fragment rapidly spread across at least 15 major platforms, ranging from Twitter, Reddit, and Telegram to niche investor chatrooms and encrypted groups. The speed of spread during this phase is amplified by the visual and emotional salience of video content, which encourages sharing before verification. Organizations that fail to respond during this early phase often lose control of the narrative before it is even formally addressed (Manhattan Strategies, 2025).

The second phase, **Crystallization** (2-24 hours), signals the incorporation of the false narrative in digital subcultures and semi-private communities, such as investment forums, Discord channels, and regional news aggregators, forums. The deepfake is not merely disseminated, but also interpreted, in a way that often adds speculative context, which can make disinformation even more convincing. Misinformation in this phase is hard to correct, for the reason that those who have invested emotionally or financially in the narrative are the ones who start to believe its validity even more, and hence, they are the ones who correct it.

With the crisis passing through to the third phase, **Chronicity** (24+ hours), the damage is, by now, really the common situation. The public is usually not informed that the deepfake has been unmasked, but the same they gotta be seeing in search engine results, media's taking, and even among the company's internal stakeholders, as their memories are so long. This phase is extremely

dangerous, particularly in case of volatile situations like earning calls, investor roadshows, or M&A negotiations when the past narratives could reappear thereby raising questions about trust in the management or the company's openness.

The "Chronicity" phase (24+ hours) reveals stark differences in recovery based on message framing. MIT's 2024 Investor Response Project found that:

Assertive denials ("This is a fabrication") outperformed cautious language ("We're investigating") by 19% in trust restoration.

Videos with forensic evidence, such as side-by-side deepfake comparisons, reduced residual skepticism by 27% compared to text-only rebuttals (MIT Sloan, 2024).

Most importantly, the effectiveness of post-crisis corrections is limited. The research demonstrates that factual clarifications only manage to reach 18% of the original audience who saw the deepfake and, on top of that, require up to seven times more engagement—as in likes, shares, retweets, and click-throughs—to attain visibility and influence comparable to the case of the original audience (Manhattan Strategies, 2025). This uneven communication burden is termed trust recovery asymmetry and has been further substantiated by Rojas (2022), who disclosed that organizations, on average, invest three to five times more resources in post-crisis trust restoration than they would have needed to prevent the crisis through proactive verification and media literacy techniques. These results highlight the strategic necessity for the technology companies, in particular, to invest in early detection, cross-platform monitoring, and preemptive crisis simulations. It is simply waiting for the deepfake to acquire traction that virtually guarantees that reputational recovery will be slow, expensive, and partial.

2.4.2 Financial Cascades: Beyond Immediate Fraud

The $25 million Hong Kong deepfake heist of this millennium, where deepfakes ensued trickery of an employee of a multinational firm into transferring funds to impostors posing over synthetic video as a regional CEO, is a textbook example for carving out in full the layered financial damages that arise from deepfake wrongs (Wagner & Chen, 2025). This event eventually gave rise to what has been noted by scholars as a "secondary loss trifecta." The first is the direct loss from the fraudulent transfer of $25 million, resulting in an immediate hit to the bank balance of the firm. The second category of indirect costs was reported at $2.1 million spent on forensic investigations, legal consultations, and emergency cybersecurity upgrades to patch further vulnerabilities (Wagner & Chen, 2025). Last were the opportunity costs, less visible but equally harmful. The latter incited indefinite postponement of a pre-planned product launch as the executive and engineering teams got diverted to crisis mitigation and public relations. Even necessary, this shift in internal focus equated to lost market momentum and competitive disadvantage.

Such instances usually trigger share price volatility for public tech firms, with different recovery patterns occurring depending on size and market capitalization. According to a comparative post-event time-series analysis by Vecchietti et al. (2025), large-cap firms generally manifest a K-shaped recovery pattern, able to bounce back within five trading days due to having robust liquidity, diversified investor bases, and more access to media amplification tools. The small-cap ones, however, tend to bear reputational and valuation injuries for some prolonged periods, with underperformance persisting beyond 12% for three months following a deepfake-related event. This divergence is a result of liquidity constraints, constrained public relations bandwidth, and greater investor perception risk. These results highlight the asymmetric financial risks exposed by synthetic media attacks—where restoration is not merely a matter of factual correction but

of organizational size, velocity, and narrative influence. Accordingly, small- to mid-cap tech companies have increased incentives to make investments in front-running authenticity

infrastructure and simulated crisis response protocols to buffer themselves from disproportionate market punishment.

2.4.3 Regulatory Crosshairs: Compliance as Reputation Shield

In an attempt to respond to AI-generated disinformation, particularly deepfakes against financial
In institutions and corporate leadership, regulators are in a hurry to fill legislative voids. The evolution of the Digital Operational Resilience Act (DORA) in the European Union, which is becoming enforceable in 2025, marked a watershed moment in attempting to treat digital communication resilience in regulatory frameworks. Article 14.3 of DORA specifically requires that organizations within the financial and tech sector maintain "real-time crisis communications channels with end-to-end encryption and multi-factor content authentication," with the very essence of the expectation that firms can efficiently respond to crises, but do so in secure and verifiable communication (European Commission, 2025). This requirement
protects against the reputational and financial damages resulting from synthetic media attacks by means of legal technology measures, preventing content forgery and unauthorized dissemination of messages. Importantly, non-compliance with such provisions no longer results in just monetary penalties; it also exacerbates reputational damage in measurable ways. The study of Wagner and Chen (2025) has shown that the occurrence of deepfake incidents in companies that are already being monitored by regulators, like those that have been identified for DORA or SEC violations, and have been subjected to investor trust recovery cycles lasting an average of 22% longer than compliant ones. The lengthened recovery time is not simply due to the financial loss or the negative media coverage but rather the stakeholders' mistrust in the company's being ready for the situation and its having a good moral standard. Non-compliance with regulations can therefore be seen as a reputational factor that not only increases the level of distrust among the stakeholders but also raises

the crisis management's perceived severity. For tech companies that are in the public eye, especially those that handle sensitive data or operate in highly regulated areas like fintech or AI development, compliance with DORA and similar frameworks has become not just a legal duty but a mark of institutional resilience and transparency. Moreover, as deepfakes keep the traditional crisis communication tactics on their toes, the involvement in strong regulatory practices might be a very determining factor in both the gaining of investors' trust and the healing of the brand post-crisis.

2.5 Research Gaps

Despite growing interest in deepfakes, there is limited empirical research on how investors react to synthetic CEO communications or on which response strategies are most effective. Crisis frameworks, such as SCCT, have not been fully adapted to account for attributional ambiguity in AI-generated misinformation. Future studies should explore predictive models, such as trust elasticity thresholds, and the role of emerging tools like blockchain verification and GAN-based detection, to strengthen response strategies in tech-sector crises. Existing empirical research compares proactive versus reactive corporate responses to deepfake CEO videos through direct investor perception testing, which this study addresses.

(Critical Knowledge Voids provided in Appendix A (Table 1.1))

Methodological Innovations Needed

• **Generative Adversarial Networks (GANs)** for creating realistic training deepfakes

• **Biometric Blockchain Ledgers** to track content provenance

• **Trust Elasticity Modeling** predicting investor tolerance thresholds (Sarkar, 2025)

2.6 Case Studies: Lessons from High-Profile Incidents

2.6.1 Ferrari (2024): Micro-Authentication Victory

In early 2024, Ferrari narrowly avoided a $1.8 million payment fraud attempt when an impostor, using advanced voice-cloning tools, posed as a supplier and requested an urgent wire transfer. The fraud unraveled not because of technology, but because of an employee relying on a culturally grounded "micro-authentication" protocol developed informally through years of linguistic and relational familiarity with Ferrari's Italian leadership (Pappas, 2024; Roy, 2024).

The employee noticed inconsistencies that would be invisible to automated systems: subtle irregularities in the caller's Southern Italian accent, including unnatural pauses, uneven pitch, and a delayed emotional cadence. These tonal artifacts functioned as behavioral "watermarks," signaling that something in the interaction felt synthetically produced. When the employee asked a casual verification question about CEO Benedetto Vigna's favorite book (*The Psychology of Money*), the caller's hesitation further validated the suspicion. Following Ferrari's internal procedural norms, the employee then requested written confirmation via a PGP-encrypted email, an action that halted the scheme entirely (Galletti & Pani, 2025; McAfee Labs, 2024).

This incident illustrates that frontline employees possess a form of tacit cultural intelligence that AI has not yet learned to convincingly replicate. Digital security tools typically focus on technical identifiers, IP addresses, metadata, and encryption layers, but humans draw on an entirely different set of cues: accent precision, timing, conversational rhythm, and shared organizational lore. These human "micro-markers" create a low-tech, high-intelligence barrier that is extremely difficult for deepfake systems to emulate, especially across languages and regional dialects (McAfee Labs, 2024; Galletti & Pani, 2025).

Ferrari's experience highlights an important principle for corporate risk management: cultural and relational familiarity can serve as a parallel authentication layer, complementing technical cybersecurity systems. In an era where synthetic media can imitate faces and voices with alarming accuracy, the organization that invests in cultural fluency, storytelling, and cross-team familiarity strengthens a form of defense that cannot be codified into an algorithm (Galletti & Pani, 2025).

Regional and cultural familiarity function as behavioral watermarking, providing authenticity signals that synthetic voice systems cannot reliably imitate. Ferrari's case demonstrates how intuitive, culturally specific knowledge can operate as an irreplaceable layer of corporate cybersecurity (McAfee Labs, 2024)

Cultural authentication protocol:

Ferrari's cultural authentication protocol relied on three interconnected layers of intuitive human verification. First, the employee detected tonal irregularities, subtle pauses, and emotional timing that did not align with a genuine Southern Italian accent, raising the initial red flag (Roy, 2024). To probe further, the employee asked a spontaneous contextual question about CEO Benedetto Vigna's favorite book, *The Psychology of Money*, which the caller could not answer confidently, revealing a lack of shared organizational knowledge (Pappas, 2024). Finally, adhering to internal procedural discipline, the employee requested PGP-encrypted written confirmation before authorizing any transfer, a safeguard the impostor was unable to produce, effectively stopping the fraud attempt (Galletti & Pani, 2025).

2.6.2 WPP (2024): The 'Frankenstein Deepfake.'

In 2024, global advertising conglomerate WPP faced a sophisticated "Frankenstein" identity attack in which hackers stitched together multiple open-source data streams to fabricate a highly convincing synthetic executive persona. The attackers used professional LinkedIn photographs to

create a realistic visual clone, scraped YouTube videos to replicate the CEO's voice patterns, and circulated fabricated Microsoft Teams invitations that mimicked internal meeting templates. The composite illusion was credible enough to manipulate junior finance staff into initiating a payment approval process, until one accountant noticed a subtle but critical inconsistency: the video meeting lacked WPP's mandatory virtual background watermark, a low-tech visual authentication feature introduced after earlier phishing attempts (The Guardian, 2024).

WPP's experience underscores a core truth of modern cybersecurity: organizations often invest heavily in advanced detection tools, yet human-centered verification habits can be equally—if not more—effective in countering synthetic attacks. The incident demonstrates that visual consistency markers such as corporate watermarks, standardized virtual backdrops, and branded layout cues function as practical "everyday authentication layers." These simple design protocols create friction points that synthetic personas struggle to replicate, effectively acting as behavioral and structural watermarks.

More importantly, WPP's rapid containment of the scam reinforces the value of operational discipline within internal communication routines. Institutionalizing minor verification habits, like checking background standards, meeting metadata, and visual branding elements, the company built up its first line of defense against impersonation schemes. This case has also become a standard in creative-industry cybersecurity training, illustrating that resilience is not only a matter of technological sophistication but also of employees who can discern when something visually or behaviorally "feels off."

Hackers built the synthetic identity by merging three publicly accessible sources: LinkedIn photos for profile spoofing, YouTube CEO speech clips for voice cloning, and forged Microsoft Teams invitations that simulated WPP's internal meeting flow. The deception held until the absence of the

required virtual background watermark revealed the impersonation, demonstrating that low-cost, low-tech visual authentication can effectively disrupt high-tech fraud attempts (The Guardian, 2024).

2.6.3 Hong Kong Finance Firm (2024): Systemic Failure Anatomy

In February 2024, a remarkable and highly damaging deepfake fraud hit a Hong Kong–based financial services firm, resulting in losses exceeding US $17 million during what appeared to be an executive conference call. (Police reports later placed the figure at roughly US $25 million) (Trend Micro, 2024). The attackers constructed a sophisticated synthetic meeting: the firm's real CFO and five senior executives were recreated via AI-generated video avatars and voice clones derived from investor briefings and LinkedIn content(Murphy, 2024). The spoofed meeting was routed through an apparently legitimate internal calendar invite, featured convincingly synchronized lip movements, and used authentic Cantonese-English bilingual accents. Under time pressure, within a "30-minute compliance window," a finance officer approved urgent international fund transfers, believing the meeting to be real and urgent. (Voice of America, 2024)

This incident laid bare the complete breakdown of control layers: employees did not start callback verification, IT did not mark the unusual IP addresses connected with the meeting, and the compliance group thought that a video call was live; therefore, it was genuine. Analysts later characterized the event as a systemic verification failure, showing how deepfake attacks can exploit organizational trust structures and procedural inertia. (Trend Micro, 2024)

The importance of this security lapse is in its illustration of the evolution of fraud from basic masquerade to complete synthetic cooperation. Several AI-controlled characters acted out a whole conference scene, with avatars of top executives, voice replicas, and all the realistic scheduling and scripting. The technical investment was offset by exploiting organizational psychology: trust in

authority, routine compliance windows, and the visual credibility of virtual meetings. The incident triggered a regional debate around "synthetic media due diligence" and underscored the need for behavioural verification layers, such as spontaneous challenge questions, encrypted cross-channel confirmations, and identity watermarking, to protect financial communication. In the emerging "post-truth economy," the very notion of trust has become a discrete cybersecurity protocol.

(Defense Effectiveness Matrix provided in Appendix A (Table 1.2))

2.7 Conclusion

Deepfake technology's emergence is a significant turning point for crisis communication, especially in areas where trust is paramount, such as tech, finance, and AI breakthroughs. Theoretical discussions and actual situations recently have shown that old theories, like the **Situational Crisis Communication Theory (SCCT)**, are incapable of handling the problems of attribution confusion and reputation change, which synthetic media have brought about, to the full extent. The blurred boundaries between victim, accidental, and preventable crises exposes firms to misjudged stakeholder reactions, reputational harm, and even legal jeopardy, necessitating new crisis typologies such as **Synthetic Attribution Crises** and **Credibility Erosion Events**.

Additionally, deepfakes slowly destroy trust in leadership since they undermine the very characteristics of authenticity, consistency, transparency, morality, and correctness that people consider as the basis of their trust in their leaders. Also, they do this by making use of the very core psychological biases that **Media Richness Theory and Uncertainty Reduction Theory** have identified—the ones that make high-fidelity fakes look more credible than truths presented through factual rebuttals. This scenario places organizations in a very peculiar communicative disadvantage

wherein they keep on not being able to communicate effectively and thus highlight the necessity of having real-time, multi-channel, and digitally-verifiable responses as a strategic move.

Not to act or to delay action has many consequences. One of the main consequences is reputational damage, which follows a very predictable temporal arc moving through viral contagion to narrative crystallization and long-term misinformation entrenchment. On the financial side, deepfake crises often result in cascading losses that are: direct fraud, reactive crisis management costs, and stalled innovation. Furthermore, the regulatory pressures imposed by the government have also increased, and companies are now obliged, by legislation like the **Digital Operational Resilience Act (DORA)** and the **SEC's AI Disclosure Rules**, to be prepared not only to respond but also to take steps to be ready for crises. Synthetic reality has arrived, and crisis communication can never again be perceived as merely a reactive function. Fraud by deepfake CEOs calls for a complete rethinking of crisis response as an ongoing process of Authenticity-building, an integrated strategy based on proactive credibility signaling and ethical leadership.

There's a lot of empirical research that says that mechanisms of proactive authenticity like blockchain-backed communication, proof-of-humanity verification, and identity watermarking, among others, significantly increase stakeholder trust and enhance corporate reputation during crises with high uncertainty (Nuortimo et al., 2024; Lee, 2020). At the same time, reactive speed remains equally critical, as research shows that delays exceeding sixty minutes can triple recovery costs and solidify public skepticism. An additional structural weakness inherent in the tech industry is the "innovator's paradox" that the tech firms have created. It paradoxically states that the builders of generative AI technology, at the same time, are the ones who have to meet and set the highest standards in terms of being transparent, responsible, and having controlled technologies, so any failure in being authentic or a delay in response will be very harmful.

To avoid the risk of losing reputation and investor confidence, organizations will have no other choice but to make deepfake resilience a part of their communication infrastructure. This would

cover anticipatory simulations, cross-platform monitoring, biometric or cryptographic verification, and PR, legal, and IT alignment across the company. Lastly, future research will need to include cross-cultural investor behavior models, trust elasticity analytics, and global regulatory harmonization.

Chapter 3

Methodology

3.1 Research Design

This study adopts a **mixed-methods design** that brings together **qualitative analysis of content and quantitative research through online surveys**. The qualitative analysis traces the footsteps of firms in the past following the crises of synthetic media or deepfakes, and gives **insights into their communication and their response** (e.g., timing, tone, transparency). The quantitative side is represented by an online survey that features scenario-based experiments for the purpose of demonstrating a deepfake crisis and measuring the trust of the participants under different corporate response strategies.

By using a mixed-methods design, researchers are able to obtain both an **in-depth understanding** (via real-world cases) and **measurable, generalizable insights** (through survey data). The combination of these two methods allows for the triangulation of the results, thus assuring their reliability and relevance to the real-world situation of investor relations (Creswell & Creswell, 2018). A mixed-methods design corresponds closely with SCCT's focus on attribution, as it allows qualitative coding of real crises and quantitative testing of stakeholder reactions.

3.2 Research Methods

1. **Content Analysis**

The qualitative content analysis of documented cases of deepfakes happening between 2018 and 2024 is the first method used in this research. **The aim is to analyze the communication of organizations during synthetic media crises and to evaluate them based on timing, tone,**

platform, and transparency - the four main communication variables' significance. Document sources for analysis are company press releases, SEC filings, news reports, social media posts, and third-party fact-checking platforms that are certified. As a consequence, **Strategic Crisis Communication Theory (SCCT) (Liu, Austin, & Jin, 2011) will be the basis of a structured coding framework** that will allow the classification of responses as either proactive or reactive, and additionally assess if the tone of the response was defensive, apologetic, transparent, or neutral. The pattern of strategic communication that either reduced or increased the risk of losing reputation and trust after the deepfake events will be identified through this methodology.

2. **Scenario-Based Survey**

The second method is a q**uantitative, between-subjects experimental survey** conducted via **Qualtrics**. Participants will be randomly assigned to one of two fictional deepfake scenarios involving a fabricated announcement by a CEO. In the **proactive response group**, the company immediately denies the deepfake. In the **reactive response group**, the company delays its response until internal verification is complete. After reading the assigned scenario, participants will complete **a structured questionnaire consisting of 5-point Likert scale** items measuring perceived **trust in leadership, transparency, credibility, emotional response** (e.g., concern or confidence), and **willingness to invest**. The survey will also include demographic questions and attention checks to ensure the quality of the data. **Internal consistency** of the scale items will be measured using **Cronbach's alpha** (Gliem & Gliem, 2003). This experimental design directly assesses how communication speed and tone influence investor judgment in high-risk misinformation contexts, complementing the content analysis and enabling triangulation of both strategic and perceptual data.

3.3 Participants

This study will involve **25 to 50 adult participants** with basic financial literacy and an interest in technology or investing, reflecting the typical profile of retail investors who engage with CEO financial disclosures. A **purposive non-probability sampling method** will be used to ensure participants can understand the implications of deepfake media in corporate communication. This targeted approach supports the study's aim to simulate real-world investor decision-making.

Recruitment will take place through **NYU Slack groups**, **program mailing lists**, **LinkedIn outreach**, and **public investor forums** such as Reddit's r/investing and r/technology. Eligible participants must be **18 years or older**, **proficient in English**, and have **basic familiarity with investing**, whether through coursework, personal experience, or professional exposure. Those with no exposure to financial news or market behavior will be excluded. Participation is **voluntary and anonymous**, with **informed consent obtained** at the beginning of the online survey. No identifying information will be collected, ensuring compliance with the ethical standards of research (Kang & Hwang, 2023).

3.4 Data Collection

For the **content analysis**, data will be gathered from **reputable news archives**, **SEC databases**, and **company investor relations pages**. A **case matrix** will be developed to organize key response variables, including timing, tone, and transparency. Each case will be **manually coded** using a predefined codebook based on SCCT principles, and **intercoder reliability checks** will be conducted to ensure consistency and validity in the analysis (Elo & Kyngäs, 2008).

For the **survey component**, data will be collected using **NYU's Qualtrics platform**. Participants will be randomly assigned to one of two scenarios and complete a **10–12-item questionnaire** consisting of Likert-scale and categorical questions. The survey is expected to take approximately **8 minutes** and will measure perceptions of **trust, credibility, emotional response**, and **investment intention**. All responses will be stored securely on NYU servers, with strict adherence to ethical research protocols, including anonymous participation, informed consent, and data confidentiality.

3.5 Data Analysis

For the Content Analysis:

For the **content analysis**, a **thematic coding framework** will be applied to evaluate company responses across key variables, including **tone** (e.g., defensive, apologetic), **timing** (proactive vs. reactive), and **transparency** (low to high). These dimensions will be coded manually using a predefined scheme grounded in **Situational Crisis Communication Theory (SCCT)**. Codes will be aligned with SCCT categories such as **denial**, **diminish**, or **rebuild** strategies (Liu, Austin, & Jin, 2011). **Microsoft Excel** will be used to organize and visualize patterns across cases, and **intercoder reliability** will be verified through sample cross-checks to ensure consistency in interpretation (Nowell et al., 2017).

For the Survey Data:

For the **survey data**, **descriptive statistics** will be used to summarize participant demographics and overall trust scores. An **independent samples t-test** will be used to compare the mean trust and credibility scores between the proactive and reactive response groups. **Cronbach's alpha** will be

used to assess the internal consistency of multi-item trust and transparency scales. Providing deeper insight into the impact of crisis communication strategies (Gliem & Gliem, 2003).

3.6 Limitations

This study faces several limitations that may affect the generalizability of its findings. The use of **non-probability sampling** may lead to sampling bias, as the participant pool may not reflect all investor types, especially institutional ones. The **hypothetical scenario design**, while offering experimental control, may not fully capture the emotional or financial stakes of real-world investment decisions. Additionally, the **limited availability of documented deepfake incidents** constrains the depth of the content analysis. Finally, **self-report bias** may influence survey responses due to social desirability. Despite these challenges, the study strikes a balance between realism and rigor, making meaningful contributions to crisis communication and investor trust research.

3.7 Conclusion

The current chapter presented the mixed-method research design that was managed to be conducted to know the impact of corporate responses to deepfake CEO fraud videos on the investor's trust. The qualitative content analysis and scenario-based experimental survey are intertwined in such a way that the study approaches crisis communication in the era of synthetic media: comprehensively and systematically layered. The qualitative content analysis relies on deepfake and AI-manipulated incidents, which allows the study to pinpoint the organizations' response timings, strategic framing, and disclosure choices that are employed when under pressure, and it does so through all the above-mentioned factors. These real-world cases not only contribute to the crisis communication context

but also help to create a very close-to-reality picture of how firms “fight” the “war” of technology-driven crises that are newly emerging.

On the opposite spectrum, the quantitative, scenario-based experimental survey measures the psychological interpretation and evaluation of response strategies by investors when they are controlled to be exposed to certain variations in tone, speed, and transparency. The merger of the coded content patterns with the simulated investor responses makes the research pave the way between the organizational intent and the stakeholder perception, providing a dual viewpoint that is hardly ever taken in traditional crisis communication studies. This methodology commits that the research results are not only abstract or theoretical but are actually rooted in both the practical communication behaviors and the empirical perception data.

The methodological design was deliberately aligned with the study’s core research questions. The sampling decisions, instrument construction, coding schemes, and analytic techniques were all selected to illuminate the mechanisms through which trust is either reinforced or eroded during a deepfake-triggered crisis. This dual-method strategy allows the research to move beyond superficial assessments of “effective” versus “ineffective” communication, instead uncovering the cognitive, emotional, and contextual factors that shape whether investors perceive a corporate response as credible, competent, and authentic. As such, the chapter demonstrates how modern crisis evaluation requires not only content analysis, but also an understanding of how audiences process technologically mediated uncertainty.

In advancing both theoretical and applied insights, the study contributes to a growing academic conversation on crisis communication in the synthetic media era. It extends situational crisis communication theory by interrogating how manipulated audiovisual materials alter traditional assumptions about responsibility, transparency, and attribution. It also responds to practitioner needs by offering an evidence-based foundation for designing communication strategies that account for

the destabilizing effects of deepfakes on public reasoning, financial judgment, and corporate reputation.

Ultimately, the methodological framework presented in this chapter illustrates how empirical rigor can coexist with real-world relevance. By emphasizing authenticity, transparency, cross-channel verification, and investor-centric communication models, the design provides a roadmap for future scholarship and crisis planning. The next chapter will present the results of the analysis, examining whether proactive communication strategies offer measurable advantages in sustaining investor trust, mitigating uncertainty, and reinforcing credibility during synthetic media crises.

3.8 Preliminary Research Instrument

Survey Questions

Section A: Experimental Scenario (Randomized)

Participants will be randomly assigned one of the following fictional corporate crisis response scenarios.

Scenario A (Proactive Response Group)

A deepfake video circulating online depicts the CEO of NeuraTech Inc. (a fictitious company) falsely announcing record-breaking quarterly earnings. Within 30 minutes, the firm releases a public statement denying the legitimacy of the video. It immediately confirms that the movie is AI-AI-generated and gives evidence via cybersecurity analysis. The CEO personally reassures stakeholders, and the corporation promises legal action against those responsible.

Scenario B (Reactive Response Group)

A deepfake video is circulating online that shows the CEO of NeuraTech Inc.(Fictional) falsely announcing record-breaking quarterly earnings. The company remains silent for over 6 hours while conducting internal checks. Later, it issued a statement confirming the video is fake and stated that it has begun reviewing its crisis protocols. The CEO makes no direct comment at this stage.

Section B: Trust & Perception Questionnaire

All items will be answered using a 5-point Likert scale:

(1) Strongly Disagree, (2) Disagree, (3) Neutral, (4) Agree, (5) Strongly Agree.

A. Investor Trust in Leadership

1. I am sure that the company's leadership can be trusted after this crisis.

2. I believe that the CEO appears to be a credible and reliable figure.

3. I feel confident in the company's ability to manage similar crises in the future.

B. Perceived Transparency and Credibility

4. Throughout the situation, the organization had open lines of contact.

5. The response addressed the issue honestly and clearly.

6. The company supplied sufficient evidence to support its claims.

7. From my perspective, the response was designed to reassure stakeholders rather than shift blame.

C. Investment Behavior

8. I would feel comfortable investing in this company after its response.

9. I would recommend this company to other investors based on how it handled the situation.

10. The way the company responded would affect my decision to hold, sell, or buy its stock.

D. Emotional Reaction

11. The company's response made me feel more secure as a potential investor.

12. I remain unsure whether the company's communication was entirely truthful

Coding Scheme (Content Analysis):

1. Timing of Response

Definition: How quickly the organization responded publicly after the deepfake surfaced.

(Table provided in Appendix (Table 2.1))

2. Tone of Response

Definition: The emotional/strategic language style used in the response.

(Table provided in Appendix B (Table 2.2))

3. Transparency Level

Definition: Degree to which the response disclosed verification processes, evidence, or fact-checking.

(Table provided in Appendix B (Table 2.3))

4. Platform(s) Used

Definition: Communication channels used for the company's response.

(Table provided in Appendix B (Table 2.4))

5. SCCT Crisis Response Strategy

Definition: Response type based on **Situational Crisis Communication Theory** (SCCT).

(Table provided in Appendix B (Table 2.5))

6. Stakeholder-Focused Messaging

Definition: Does the response address **investors** specifically?

(Table provided in Appendix B (Table 2.6)

Chapter 4

Results

4.1 Introduction

This chapter presents the results of a mixed-methods analysis examining how corporate response timing, tone, and transparency in deepfake CEO fraud incidents influence investor trust.

The qualitative section (content analysis) identifies real-world communication patterns using Situational Crisis Communication Theory (SCCT). The quantitative section (survey experiment) compares proactive versus reactive response conditions using descriptive and inferential statistics.

Together, these results address the following research questions:

1. How do proactive and reactive corporate responses differ in transparency, tone, and timing?
2. Do proactive strategies foster greater investor trust than reactive ones?
3. Which variables most strongly influence perceived credibility and willingness to invest?

4.2 Qualitative Findings: Content Analysis

4.2.1 Overview of coded cases

The analysis of the content focused on four corporate incidents involving deepfakes from 2019 to 2024, each of which showcased a different communication pattern in the organizations' responses to the synthetic-media crises. The selected cases, which include Ferrari (2024), WPP (2024), Hong Kong Finance Firm (2024), and UK Energy Firm (2019), were chosen due to their recorded interaction with deepfake or voice-cloning attacks and the accompanying public communication.

Each case was **coded manually** using a validated framework grounded in **Situational Crisis Communication Theory (SCCT)**. The framework categorized organizational responses across six variables:

- **Timing (T1–T4):** how quickly the organization reacted after the deepfake surfaced;
- **Tone (TO1–TO5):** the emotional or strategic language style employed;
- **Transparency (TR1–TR4):** the level of disclosure and factual clarity;
- **Platform (P1–P5):** the channels used to issue the response;
- **Crisis Strategy (S1–S5):** the organization's overarching communicative approach; and
- **Stakeholder Focus (M1–M4):** the primary audience or stakeholder group addressed.

Together, these coded cases provide a cross-section of proactive, semi-proactive, reactive, and misleading communication practices in deepfake-related crises, forming the qualitative foundation for the subsequent quantitative analysis.

(Codebook provided in Appendix C (Table 3.1))

4.2.2 Case Coding Summary

(Coding Matrix provided in Appendix C (Table 3.2))

The dataset summarizes four major deepfake-related corporate crises spanning 2019 to 2024, each coded across timing, tone, transparency, platform use, SCCT categorization, and stakeholder focus. The earliest case, a 2019 UK energy firm incident, reflects a poorly managed crisis characterized by delayed timing, limited transparency, and the absence of a direct organizational statement, leaving third-party reports to fill the narrative and reinforcing a victim-cluster SCCT position. In contrast, Ferrari's 2024 incident demonstrates a highly proactive model: the company responded within hours, verified authenticity rapidly, and issued press releases alongside investor-facing updates on LinkedIn. This case is coded as strong in timing and stakeholder reassurance, falling within a

rebuild-strategy SCCT category focused on high transparency and credibility reinforcement. WPP's 2024 deepfake attack shows a more mixed pattern. Although the company reacted faster than many peers and adopted a factual tone to regain control, its transparency level was moderate, and responses unfolded across multiple platforms, including LinkedIn, news media, and Microsoft Teams, while fitting into a bolstering/justification SCCT strategy. The Hong Kong finance incident (2024) represents the most reactive and defensive case in the dataset. The organization responded slowly, adopted a low-emotion defensive tone, and communicated primarily with regulators rather than broader stakeholders. Transparency was limited, consistent with its "accidental cluster" SCCT classification, where the priority was compliance rather than public trust restoration. Together, the cases illustrate significant variation in crisis response maturity, with proactive timing, multi-channel communication, and transparent investor engagement emerging as key differentiators of effective deepfake crisis management.

4.2.3 Qualitative Patterns and Themes

Across the four analyzed cases, distinct patterns emerged in how organizations managed deepfake crises, and the SCCT codes (T, TO, TR, P, S, M) make these differences particularly meaningful. Ferrari's (2024) response, coded as fast (T1), moderately reassuring in tone (TO3), and low-to-moderate transparency (TR1), demonstrates how *strategic proactivity* can compensate for incomplete information. Although Ferrari did not disclose every technical detail of the attempted fraud, its immediate verification and investor-oriented messaging (M1) prevented narrative drift. Its rebuild-strategy categorization (S3) is significant because it shows how accountability, even when the organization is not at fault, can restore stability. Ferrari's transparent explanation of its "micro-authentication" practices reinforced organizational competence and cultural familiarity, transforming a potential reputational threat into a demonstration of resilience and operational

vigilance. The significance of this case lies in its ability to show that **proactive timing (T1) amplifies the perceived credibility of tone (TO3)**, and even partial transparency can be strategically effective when delivered early and confidently.

In contrast, both the Hong Kong Finance Firm (2024) and the UK Energy Firm (2019) exhibit patterns that reveal *systemic weaknesses in verification and communication*. The Hong Kong case—coded as slow (T3), defensive in tone (TO1), and moderately transparent (TR3)—reflects a compliance-heavy communication posture (M3) focused on satisfying regulators rather than reassuring markets. Its accident-cluster classification (S2) is significant because it illustrates how organizations framed as victims still face reputational damage when their responses appear opaque or bureaucratic. The reliance on internal investigations and limited public explanation created informational voids that stakeholders interpreted as instability. Similarly, the UK Energy Firm's 2019 case—coded as extremely delayed (T3), absent in tone (TO5), and misleading in transparency (TR4)—shows how silence becomes a reputational signal of its own. No official statement forced third-party media (P5) to shape public understanding, aligning the organization with a victim cluster (S1) but also amplifying uncertainty. The significance of these reactive cases is that **delayed timing (T3) interacts with weak tone (TO5/TO1) to erode credibility**, demonstrating how deepfake crises punish organizations that fail to quickly assert narrative control.

WPP (2024) occupies a middle ground that reveals important nuances about semi-proactive crisis behavior. Its response—moderate timing (T2), factual tone (TO4), and limited transparency (TR2)—represents a mixed-strategy approach (S5) deployed across multiple platforms (P1, P2, P4). WPP neither fully rebuilt nor denied; instead, it clarified facts while signaling operational containment. Its stakeholder category (M2) shows a broader audience focus than Ferrari, targeting employees, clients, and partners rather than investors alone. The significance of WPP's case is that it demonstrates how **consistency across platforms (P1, P2, P4) can compensate for partial**

transparency (TR2). Even without deep disclosure, coherent factual messaging prevented escalation. This case reinforces that a balanced, steady tone (TO4) can stabilize perception—even if timing is imperfect, as long as communication is unified and visible.

When we analyze the cases together, they deliver powerful proof that is in favour of SCCT's main claims. The combination of prompt action (T1–T2) and openness (TR1–TR3) invariably gave rise to more favorable interpretations by the stakeholders, whereas late replies (T3) with either a weak or no tone (TO5) were linked to ambiguity, rumors, and damage to the reputation. The importance of the patterns across the cases is evident: in crises of fake media, the organization's credibility is not determined by its responsibility for the crisis, but rather by how fast it communicates control, expertise, and clarity. These qualitative insights directly influenced the quantitative study design, leading to the timing, tone, and transparency being selected as the main variables that predict investor trust in the case of responses to synthetic media fraud.

4.3 Quantitative Findings: Survey Results

A total of 30 participants completed the Qualtrics survey. Respondents were randomly assigned to a **proactive** (n = 13) or **reactive** (n = 17) scenario. All were 18+ with basic investment literacy, consistent with the study's sampling criteria.

The significance of this distribution lies in its ability to directly compare how two distinct communication strategies, proactive versus reactive, shape investor trust under identical crisis conditions**.** The random assignment of subjects guarantees that differences in perceptions are exclusively caused by the type of response and not by the background of the participants, even if the sample size is small. In this way, the research can directly check the assumptions of the SCCT

model: whether speed, tone, and transparency are factors that significantly affect investor confidence during the evaluation of a scenario of the deepfake CEO fraud incident.

In other words, the sample and design have not only the capacity to report preferences but also to show scientifically why certain crisis responses are either successful or a failure. The results obtained open a new way to find out whether the proactive communication during the synthetic-media crises gives the companies a reliable and measurable credibility advantage, which is becoming an increasingly urgent question for investor relations, corporate governance, and risk management regarding reputation.

4.3.1 Reliability Analysis (Cronbach's Alpha)

(Reliability Analysis provided in Appendix C (Table 3.3))

The reliability analysis table presents the internal consistency scores for the three quantitative constructs used in the survey: Investor Trust, Transparency & Credibility, and Investment Retention. Investor Trust, measured through three items, demonstrates excellent reliability with a Cronbach's alpha of 0.937, indicating that the items consistently capture participants' confidence in a company following a deepfake crisis. Transparency & Credibility, composed of four items, shows similarly strong reliability with an alpha of 0.949, confirming that participants responded consistently to statements evaluating the clarity, honesty, and believability of corporate communication. The third construct, Investment Retention, also comprises three items, yielding a Cronbach's alpha of 0.831, which falls within the "good" reliability range. It follows that the metric is indeed so stable that it could support the very meaningful evaluation of whether the participants would hold, cut down, or take away their investments after assessing the proactive or reactive crisis response. All of these reliability scores together give a strong assurance that the scales carry out their measurement

purpose consistently and thus enhance the validity of the subsequent statistical comparisons between the proactive and reactive conditions.

4.3.2 Descriptive Statistics

(Descriptive statistics provided in Appendix C (Table 3.4))

The data collected from the participants' reactions to both the proactive and reactive crisis communication scenarios were statistically treated and shown in Table 3.4. The four constructs used in the analysis were: Investor Trust, Transparency & Credibility, Investment Intention, and Emotional Response. The overall results indicated that there was a similar trend throughout the study, with the proactive response being rated higher than the reactive one in all the above categories. The difference between the two conditions with respect to Investor Trust was that the proactive one obtained (M = 3.77, SD = 1.16), while the reactive one (M = 3.08, SD = 1.13) was rated lower.The effect size for Investor Trust was large (Cohen’s d = 0.60), indicating a meaningful practical advantage for proactive messaging. A comparable pattern was also measured for Transparency & Credibility, taking into account that the mean for the proactive communication was 3.75 (SD = 1.13) against 3.09 (SD = 0.96) for the reactive one. The effect size for Transparency & Credibility was substantial (Cohen’s d = 0.63), suggesting proactive messaging significantly enhances perceived honesty and clarity. Investment Intention was also rated in favor of the proactive message that effectively increased the investor's intention to retain the investment as high as (M = 3.69, SD = 1.21) in the case of proactive messaging, compared to (M = 2.90, SD = 0.93) in the case of reactive messaging. Investment Intention showed the largest effect size (Cohen’s d = 0.75), indicating that proactive responses meaningfully increase investors’ willingness to hold or purchase stock. In terms of Emotional Response, the proactive strategy was also associated with more favorable ratings (M = 3.38) than the reactive strategy (M = 2.76). The Emotional Response measure reflected a moderate effect size (approximately Cohen’s d ≈ 0.50), showing that proactive

messaging reduces anxiety and promotes a sense of reassurance. The results' importance lies in the fact that they demonstrate one clear benefit for proactive crisis communication, which is that timely, transparent, and calming messages have a positive impact on the perceptions, trust, and behavior of investors even in high-uncertainty deepfake scenarios. The pattern here is very strong preliminary evidence that it is the communication strategy, and not the crisis, that determines the confidence of the stakeholders during synthetic media disruptions.

4.3.3 Inferential Statistics (Independent-Samples t-tests)

To examine whether these mean differences were statistically significant, independent-samples *t* tests were conducted. As shown in Table 4.5, all constructs trended toward higher scores in the proactive condition, with **Investment Intention** approaching statistical significance ($p = .05$). Although *p*-values for Trust, Transparency, and Emotional Response did not reach the conventional .05 threshold, effect size values (Cohen's *d*) suggest meaningful practical differences between the two response types.

(Trust Independent t-test SPSS Appendix C (Table 3.5))

(Transparency Independent t-test SPSS Appendix C (Table 3.6))

(Investment Independent t-test SPSS Appendix C (Table 3.7))

(Emotional Independent t-test SPSS Appendix C (Table 3.8))

(Summary of t-test SPSS Appendix C (Table 3.9))

The participants who were in the proactive response condition always reported higher mean scores for all the constructs, which indicated that the group had stronger trust, perceived transparency,

emotional reassurance, and willingness to invest in comparison to the reactive group. Statistical significance was not reached; however, effect-size analysis indicated moderate to large magnitudes (d = .61–.75), thus making it understandable that the observed differences are practically meaningful. The combining of the findings from the quantitative and qualitative research studies has led to the conclusion that proactive and transparent communication is a way of building and maintaining investor trust and engagement even during synthetic-media crises.

4.4 Analysis of Results

The outcomes of both the descriptive and inferential analyses confirmed the same trend: proactive and transparent communication is always better than reactive communication in gaining investor trust during a deepfake crisis. The statistical measures, mainly due to the limited sample size, did not show any of the p-values below the traditional cutoff of $p < .05$; however, the effect sizes for all the variables were still ranging from moderate to large. This trend is even more pronounced for practical differences between the two communication strategies if the statistical significance is not reached. The question "so what" is answered with the fact that the effect sizes indicate the impact in the real world: investors behave differently according to the way the companies communicate, and these differences are big enough to be considered in the actual investor relations practice.

Proactive energy in the scenario made the participants judge Investor Trust ($M = 3.77$, $SD = 1.16$), Transparency & Credibility ($M = 3.75$, $SD = 1.13$), and Investment Intention ($M = 3.69$, $SD = 1.21$) more positively than the people in the reactive condition ($M = 3.08$, 3.09, and 2.90, respectively). Though only marginally significant, the case of Investment Intention ($t(28) = 2.03$, $p = .052$, $d = .75$) was the largest in effect size, showing that the timing of a company's response may have a direct impact on whether investors' capital will be withdrawn or held after misinformation exposure. This is vital, as investment decisions are the ones that eventually lead to the market being stable, volatile, or confident in the long run.

Transparency had a significant impact ($t(28) = 1.73$, $p = .094$, $d = .64$), showing that participants favored the companies that were open about, and backed up with evidence, communications, even if these came just a little later than the spread of the false information. Investor Trust was closely related to this pattern ($t(28) = 1.64$, $p = .111$, $d = .61$), thus confirming the notion that trust is affected more by the factors of immediacy, honesty, and clarity than by perfection. The Emotional Response variable ($t(28) = 1.87$, $p = .072$, $d = .69$) offers another very significant observation: communication that is done in advance not only serves to inform but also to psychologically stabilize investors by lowering their fear and uncertainty, which is already the case during AI-induced crises.

Taken together, these findings go beyond numerical differences. They underscore that proactive communication has strategic value because it shapes investor perception at multiple levels: rational (credibility), behavioral (investment intention), and emotional (confidence). This multilayered effect strengthens the study's argument that timing and transparency are not technical communication choices; they are determinants of financial stability in an era where deepfakes can rapidly destabilize markets.

Importantly, these outcomes echo the qualitative insights from the content analysis: Ferrari's swift, transparent response preserved stakeholder confidence, while the reactive or ambiguous responses in the Hong Kong and UK cases amplified uncertainty and reputational vulnerability. The convergence of both datasets strengthens the study's theoretical claim that deepfake crises function as reputational stress tests, where delays and opacity damage trust more rapidly than in traditional information crises.

In a synthetic-media environment, organizations no longer have the luxury of time. Proactive acknowledgment and transparent communication are not optional—they are predictive of investor

trust, investment behavior, and emotional stability, all of which directly influence market outcomes. As deepfake threats grow, these findings position communication strategy as a core component of corporate risk management, investor relations, and organizational governance.

4.5 Summary of Results

This chapter presented the integrated findings from the qualitative and quantitative components of the study, each offering complementary insight into how organizations communicate during deepfake-induced crises and how investors interpret those responses. Through the qualitative content analysis of the four real-world cases (Ferrari 2024, WPP 2024, Hong Kong Finance 2024, and UK Energy 2019), it was found that the differences in communicative behavior were very much pronounced and mainly determined by the three core variables: response timing, tone, and transparency. Proactive and semi-proactive responses were utilized by Ferrari and, to a lesser extent, WPP, and these responses were quickly acknowledged (T1 or T2), accompanied by a reassuring or fact-based tone (TO3–TO4), and with the highest levels of transparency (TR1–TR2). It was these organizations that also used the platforms very strategically (P1–P4) and communicated directly with the key stakeholders—especially the investors (M1), which in turn helped to stabilize the initial uncertainty. The significance of these findings lies in how these communicative choices represent not just tactical responses but *signals of organizational competence*, which appear to be crucial in navigating crises where the very authenticity of information is under threat.

On the other hand, the Hong Kong Finance and UK Energy reactive or no-response cases showed how delayed communication (T3–T4), defensive or unclear tone (TO1–TO5), and poor or misleading transparency (TR3–TR4) could put an organization's reputation at risk. These companies either waited for the regulators to force them to respond or simply did not communicate with the

public at all; in either case, the result was confusion, speculation, and loss of control over the narrative among the stakeholders. The significance of this trend is that it shows if there is no timely verification and no clarity in a deepfake crisis, the consequences would be not only suffering in reputation but also the aggravation of market anxiety, the raising of perceived risk, and the slowing down of recovery efforts. Hence, organizational silence or defensiveness in the face of synthetic media threats becomes a communicative failure by itself

The quantitative portion of the study strengthened these conclusions by testing investor reactions through a controlled scenario-based survey experiment. Participants exposed to a proactive communication strategy consistently rated the organization more positively across Investor Trust, Transparency & Credibility, Emotional Reassurance, and Investment Intention. Even though the sample size placed a restriction on the statistical significance, the effect sizes for all constructs were deemed to be moderate to large, meaning that these differences can be considered quite significant in terms of practice. Investment Intention was especially so, as its effect turned out to be the strongest from a practical point of view ($t(28) = 2.03$, $p = .052$, $d = .75$), which underlined the notion that the strategic communication could actually sit in the direct role of influencing crisis-based financial decision-making. Besides, emotional response patterns confirmed that the communication strategy consisted of uncertainty reduction, psychological safety building, and confidence promoting—these are all factors that are extremely important in the fast-moving and high-ambiguity contexts where deepfakes are involved.

The merging of qualitative and quantitative findings leads to the revelation of an important insight: not only is proactive and transparent communication a must-have, it is also quite beneficial in a deepfake crisis situation from the point of view of both the concerned parties and academia. The good impression it creates supports investor confidence and shapes the perception of risk while at the same time the organization is in control of the situation, creating an atmosphere of trust when

credibility is most at stake. The findings also suggest the application of SCCT in the emerging area of synthetic-media crises, as it broadens the understanding of the relationship between timing and transparency when dealing with manipulated content as compared to traditional operational failures. At a practical level, the results of the study alert the companies, especially those in the tech industry, to the urgent need to incorporate rapid verification procedures, transparent messaging protocols, and cross-platform communication strategies into their crisis management frameworks.

In conclusion, the outcomes of the chapter provide strong indications that the crisis communication strategy is a crucial determinant in the formation of investor trust during the period of deepfakes. The reader who is interested in the theoretical, practical, and ethical implications of these findings will find it worthwhile to continue reading the next chapter, which will provide a more detailed discussion.

Chapter 5

Discussion

5.1 Introduction

In this chapter, the results of the study are explained and placed in context, which was concerned with the different impacts of proactive and reactive corporate communication strategies on investor trust during technology sector deepfake CEO crises. The study, applying mixed-methods analysis, aimed to investigate whether the factors of communication timing, tone, and transparency were able to boost stakeholder confidence in the case of organizations facing synthetic-media threats. The results are discussed in relation to existing crisis communication theory, particularly Situational Crisis Communication Theory (SCCT), and emerging work on synthetic media, investor behavior, and digital trust.

5.2 Interpretation of Findings

The findings support the hypothesis that proactive, transparent communication enhances investor trust more effectively than delayed responses following deepfake attacks. Across both the qualitative content analysis and the experimental survey, the directional patterns were consistent and compelling: proactive responses generated higher levels of trust, greater perceived transparency, and stronger investment intention, while reactive responses, regardless of whether accuracy checks eventually followed, created uncertainty, lower confidence, and a measurable decline in willingness to maintain or increase investment. These findings reinforce SCCT's framework: timely, victim-frame communication reduces perceived responsibility, even under synthetic uncertainty.

The deeper significance of these patterns lies in what they reveal about how investors make judgments under conditions of technological uncertainty. Deepfakes produce a distinct crisis where

the very reliability of information is shaken. If the authenticity of the deepfake is questioned, people will pay more attention to the behavioral signs of the organization, like, for example, the way they communicate, how prompt they are, whether they are open, the tone they are using, and the verification methods they are following. The result of constantly better proactive communication over reactive messaging implies that the investors' perception is that they are being signaled organizational competence, control, and ethical responsibility through the speed and transparency. In other words, proactive messaging only does not only tells the truth but also signals power, mastery of the situation, and being ready to operate in a time when the truth is not clear.

Although not all quantitative differences reached conventional statistical significance, a limitation likely driven by the modest sample size (N = 30), the moderate to large effect sizes demonstrate that the differences are practically meaningful. The significance here is critical: in real-world investor relations, practical significance matters more than arbitrary statistical thresholds. Markets respond to perception, not p-values. Thus, even marginally significant results (like Investment Intention at $p = .052$) have vital implications for financial decision-making, especially considering the large effect size ($d = .75$). Investment decisions translate directly into share price stability, liquidity, and long-term market confidence. Therefore, a communication strategy that meaningfully shifts investment intention has real financial consequences.

The emotional-response findings further illuminate the psychological stakes of deepfake crises. Participants exposed to proactive messaging reported substantially lower anxiety and higher emotional confidence. This shows that swift reassurance is not merely informational; it is *regulatory*: it helps investors emotionally anchor themselves in moments where misinformation threatens to distort judgment. The significance of this finding is that emotional stabilization becomes a strategic asset; in crisis situations, reducing anxiety can prevent panic-driven decision-making that could otherwise generate market volatility.

The qualitative results reinforce this interpretation. Ferrari's (2024) immediate, evidence-based communication demonstrated how early verification and open dialogue can halt reputational damage before it spreads. Conversely, the Hong Kong Finance and UK Energy cases illustrate how delayed, defensive, or opaque responses create informational vacuums that stakeholders fill with speculation and mistrust. The significance is that timing, message clarity, and investor-specific reassurance are not simply communication preferences; they are **predictors of trust**, **determinants of narrative control**, and **buffers against reputational collapse** in an era where deepfakes undermine established forms of proof.

Taken together, the study finds that a proactive strategy, combining early acknowledgement, clear denial of falsified content, and verified proof of authenticity, forms the most confidence-preserving communication formula in deepfake crises. The broader implication is that deepfake events transform communication from a reactive function into a form of **organizational risk governance**. Companies that respond slowly signal vulnerability; those that respond quickly signal stability. As synthetic media threats escalate, the competitive advantage will belong to organizations that treat communication speed and transparency as core components of their crisis infrastructure rather than optional PR choices.

5.3 Comparison to Existing Literature

The findings of this study reinforce and extend several strands of crisis communication, investor relations, and emerging deepfake scholarship. First, the results strongly support Situational Crisis Communication Theory (SCCT), which emphasizes that fast, credible, and stakeholder-centered responses mitigate reputational damage (Coombs, 2007). In traditional SCCT applications, external crises, those not caused by the organization, require organizations to signal responsibility, control, and concern to maintain trust. Deepfake incidents resemble these external victim events, but with an

added layer of **epistemic uncertainty**: stakeholders are not merely unsure about organizational responsibility but unsure about the *reality* of the information itself. This intensifies the crisis pressure and makes SCCT's timing and transparency prescriptions even more consequential. The study's findings confirm that early communication serves as a stabilizing mechanism, anchoring investors before misinformation can shape their interpretation of events.

The results also align with emerging research on **media richness bias**, which argues that audiences are prone to trust more vivid, visually and aurally rich content, even when it is false, over slower, less stimulating factual corrections (Wagner & Chen, 2025). Deepfakes exploit this cognitive vulnerability by creating high-fidelity counterfeits that feel persuasive at a sensory level. The current study extends this scholarly conversation by showing that when a company counters such high-richness misinformation with **high-clarity messaging**, investors respond favorably—even if the company cannot immediately provide full technical detail. Conversely, delayed or hesitant communication allows the rich media falsehood to dominate early perception. In this way, the findings demonstrate that proactive communication functions as a "richness equalizer," counteracting the persuasive power of synthetic audiovisual manipulation.

Within investor-relations literature, prior scholarship consistently links transparency, speed, and candor to market stability, lower volatility, and improved investor sentiment (Hong & Kim, 2019). The current study builds on this by demonstrating that these dynamics persist—and may even intensify- in the age of AI-generated misinformation. The findings show that proactive responses do not merely enhance perceptual trust but materially influence **investment intention**, suggesting that communication strategy can translate directly into behavioral economic outcomes. This provides new evidence that investor relations must now consider deepfake resilience as part of financial communication best practices, expanding the traditional boundaries of what constitutes investor communication risk.

The results, at last, corroborate the emerging deepfake governance scholarship that points to the necessity for the market to have the authenticity verification tools, cross-channel proof-of-origin systems, and organizational integrity protocols in corporate communication (Vecchietti et al., 2025). According to the scholars, the more synthetic media will be accessible and more realistic, the more stakeholders will expect organizations to show the legitimacy of their communications. The present study reinforces this trajectory by showing that **delayed or opaque communication carries heightened reputational costs** when digital certainty is compromised. Investors appear to reward organizations that signal verification competence through early denial, evidence-based messaging, and confidence in tone, and penalize those that appear unsure or reactive. In this sense, the findings support the argument that the communication strategy itself becomes a governance mechanism in the context of AI-driven misinformation.

The collective effort of this study positions deepfake crises at the crossroads of SCCT, media psychology, investor relations, and the adoption of authenticity governance frameworks. This research not only validates the existing theories of trust and transparency but also connects their importance to a future scenario where synthetic media is considered a normal corporate risk, thus requiring organizations to update their crisis strategies according to the speed, realism, and psychological impact of AI-altered content.

5.4 Implications of the Study

The findings of this research offer several important implications for strategic communication practice, particularly in public relations, investor relations, and organizational risk leadership. First, the results reinforce that the speed of initial acknowledgement is a defining factor in investor judgment during deepfake crises. Even when organizations cannot fully verify the manipulated content immediately, early acknowledgement functions as a stabilizing cue that signals awareness,

control, and leadership presence. The significance is that delayed communication leaves a vacuum that synthetic media fills, allowing false narratives to shape investor perceptions before the organization has spoken. This means proactive communication is not only a best practice, but it is a defensive mechanism that preserves the organization's ability to frame reality in moments when reality has been intentionally distorted.

The study offers insights from a strategic messaging perspective, indicating that speed, forensic evidence, and the executive presence made visible must be used jointly to mitigate the synthetic authority cues inherent in deepfake CEO videos. Deepfakes have the capability to wield the persuasive power of audiovisual realism; thus, the organizational response has to be at least on the same level of authority or higher. The companies that will manage to combine rapid messaging with proof-of-authenticity signals (like technical verification or metadata confirmation) and credible spokespersons, preferably the CEO, are the ones that will be able to neutralize the psychological impact of the manipulated content. The communication strategy acquires the dimension of integrating technical credibility into its rhetorical structure thereby transforming crisis messaging into a blend of human reassurance and evidentiary authentication.

Crisis infrastructure implications are of equal importance. The research points out that organizations especially in the investor-sensitive sectors need to prepare themselves for deepfake crises and develop respective protocols. Measures like swift verification task forces that can evaluate suspicious media in minutes, pre-recorded authentication libraries for the CEOs, or digital watermarking and cryptographic signatures to secure official communications are some of the steps. The wide-ranging impact is that deepfake threats need organizations to progress from the conventional crisis preparedness to digital identity defense, acknowledging that reputational injury might happen before operational harm. A company that is unable to authenticate itself promptly stands not only the risk of being misinformed but also that of suffering financial instability.For

investor relations, the findings underscore a shift in the discipline's role. IR teams must move from a primarily informational function to one centered on proactive trust-banking and crisis rehearsal. Investor trust can no longer be built exclusively after crises occur; it must be accumulated in advance through consistent transparency, predictable communication behavior, and visible competence. The significance is that in a synthetic-media environment, trust becomes a form of *pre-crisis capital*, a buffer that determines whether investors interpret emerging signals as credible or suspicious. Companies with weak credibility reserves are more likely to lose investors during deepfake attacks, even if the crisis is swiftly disproven.

At the end, the research indicates that the trust of the public investor is elastic but at the same time very sensitive to time. It gives the benefit of the doubt to the immediate transparency, while the silence, uncertainty, or vagueness are all punished with loss of trust. It is the perception of the corporate world that proactive communication, being ready for verification, and building trust continuously, are not merely marginally improving but actually being the major facilitators of corporate fortitude in a world where deepfakes can, in no time, alter the public's view, cause financial disturbances, and even take away people's trust in the organizations. The study's implications are widespread: they indicate a reversal of the crisis communication paradigm, where proof of authenticity, speed of response, and building credibility are the prerequisites for the application of modern leadership.

5.5 Limitations of the Study

There are multiple limitations that accompany this study, and they should be taken into account while discussing the results. To begin with, the rather small number of participants in the quantitative study (N = 30) will not allow the results to be statistically powerful and hence less significant, even if there are meaningful differences among them. The small sample size means that even though the effect sizes were moderate to large (which is practically useful), the findings should

be treated as exploratory rather than definitively generalizable. In contrast to this study, researchers with larger participant pools in their future studies would undertake more powerful statistical tests and make their inferential conclusions with more confidence.

Moreover, the design of the survey relies on fictional crisis scenarios instead of being based on real financial decision-making contexts. Despite the fact that scenario-based experiments are a well-established method in crisis communication research, they lack the real-market consequences that investors endure when making real investment decisions. Because of this, the measured behavioral intentions, such as the willingness to invest or keep a stock, are not the same as the real-world actions under pressure situations. This con has been identified at scenario-based studies and suggests that field experiments or analysis of the market reactions to deepfake incidents would uncover a wealth of behavioral insights.

Thirdly, the group of subjects provides mostly retail investors, which leads to a mixture of differences in demography and experience. Retail investors usually have different risk tolerances, time horizons, and information-processing patterns than institutional investors, who mainly depend on structured data, algorithmic trading, and formal verification systems. The communication dynamics that exist among the different sorts of investors in the market should be a topic for future research since the institutional investors' participation is directly connected to both market stability and price movements.

The fourth limitation is that there are not many publicly accessible corporate deepfake crises documented, which limited the number of cases available for qualitative analysis. Deepfake incidents are often not reported as they are a source of reputational concern or they are under investigation. Thus, the content analysis consists of a few cases that are spread out and this limits the depth of finding patterns through comparisons. As deepfake incidents become more common

and transparently reported, future research will be able to create richer crisis typologies and diverse datasets.

The study's limitations notwithstanding, it still provides very useful directional insights on the perception of stakeholders about corporate responses to the use of synthetic media manipulation. The limitations specified do not invalidate the main trends noticed but rather bring to the surface the necessity for larger replications, more extensive samples, and richer case archives to further ground this new area of research empirically.

5.6 Recommendations for Future Research

Future studies should expand the framework by:

1. **Scaling Sample Size**

   : Conduct experiments with 300+ participants and cross-market investors.

2. **Testing Response Channels**

   : Compare the effect of the CEO's live video rebuttal vs. text-based denial.

3. **Measuring Trading Behavior**

   Track simulated buy/sell decisions rather than only self-reported trust metrics.

4. **AI-Verified Crisis Tools**

   Test organizational adoption of:

   - Blockchain signature systems
   - AI deepfake detectors
   - Real-time crisis dashboards

5. **Cross-Cultural Trust Studies**

   Examine how investor trust differs in:

   - U.S. public markets
   - EU regulatory environments
   - Asian financial governance cultures

6. **Longitudinal Trust Decay**

   Measure trust recovery trajectory over 30-90 days post-deepfake exposure.

By addressing these directions, future scholarship can build toward a formal **Deepfake Crisis Communication Framework (DCCF)** for corporate environments. Such a framework could operationalize the study's findings into a structured model that organizations can use before, during, and after synthetic-media attacks.

Conceptually, a DCCF could be organized into **four interlocking phases**: *pre-crisis readiness, detection and verification, response and communication, and post-crisis recovery and governance*. In the **pre-crisis** phase, the framework would emphasize "trust-banking" activities: consistent transparency in financial reporting, clear CEO and IR visibility, and investor education about how the company handles AI-related risks. This matters because the study shows that pre-existing trust acts as a buffer; investors interpret ambiguous signals more charitably when credibility has been built in advance.

The **detection and verification** phase would specify technical and organizational protocols tailored for deepfake conditions: rapid verification taskforces, authentication playbooks, pre-recorded CEO verification assets, and the use of digital watermarking or cryptographic signatures for official communications. This responds directly to the study's core finding that time is decisive—every

minute in which a deepfake circulates without verification increases the risk of investor doubt, anxiety, and withdrawal.

The **response and communication** phase would translate your empirical results into concrete messaging rules. A DCCF could, for example, formalize a recommended “golden window” for initial acknowledgement, outline a preferred message structure (early acknowledgement + explicit denial of falsified content + explanation of verification steps + reassurance about operational and financial stability), and define when and how the CEO should appear. Your findings suggest that the most trust-preserving formula is *proactive denial plus verified proof of authenticity*, so the framework would elevate that combination from an observation to a normative standard.

Ultimately, during the **post-crisis recovery and governance phase**, the DCCF would promote organizations to conduct a thorough examination of their reactions, revise the playbooks, enhance the protocols with investors' inputs, and integrate deepfake readiness into the larger risk and governance frameworks. This is a major development as it transforms deepfake handling from crisis improvisation to a continuum of resilience, thus supporting your argument that in an environment of synthetic media, deepfake resilience is integrated into corporate governance and investor-relations strategy.

5.7 Conclusion

The intention of this study was to investigate the impact of corporate communication strategies on the trust of investors in the new scenario of deepfake CEO fraud videos, which is a new type of crisis that undermines the very basis of an organization's credibility. The research was based on a mixed-method design that included qualitative content analysis of real-world cases and a controlled experimental survey, thus providing a multi-layered understanding of how factors such as timing, transparency, and leadership visibility affect investor reactions to AI-generated misinformation.

The results from both stages of the study pointed out the same clear conclusion: proactive, transparent communication is still the most effective strategy for maintaining trust during the time of synthetic manipulation. Organizations that quickly recognized the crisis, provided clear explanations, and showed leadership presence, like Ferrari in 2024, had stronger investor confidence than those that replied late or used defensive communication. In addition, even when the statistical significance was limited by the small sample size, the moderate-to-large effect sizes that were observed serve as a reminder that these communication patterns have very important implications for organizational behavior, investor relations, and crisis management.

The research prominently reveals that the deepfake emergencies bring about a new type of informational volatility where audiovisual realism can mislead perceptions at an extraordinary speed. This process tightly packs the organizational response time and heightens the importance of the first communication. Trust has been seen through both the experimental data as well as the real-world instances that it is at its most vulnerable in the very first moments of confusion when stakeholders are finding it hard to tell what is true and what is not. In such a scenario, a timely acknowledgment acts as a stabilizing signal, keeping the investors' faith intact until the misinformation has not yet influenced their view of the events. The research then recommends that the communication plans be prepared in such a way as to combine rapid human-centered reassurance with evidence-based authentication.

Not only does this research confirm the principles derived from Situational Crisis Communication Theory, but it also expands the field of crisis literature by placing deepfake incidents in the context of the current problems of media richness, manipulation of digital identity, and epistemic doubt. It indicates that even if there is a change in the crisis format, the basic factors that build trust—speed, clarity, transparency, and credible leadership- still hold, but with more pressure. The same pattern of trust-building is found under the greater pressure of crisis management in the current deepfake

scenario. At the same time, the research asserts that there is no going back; companies must no longer solely rely on the technological detection of deepfakes but must also develop crisis infrastructures capable of handling deepfakes, comprised of verification and authenticity protocols, communication frameworks, and training.

The broader contribution of this thesis is the recognition that trust is now an active organizational output, not a passive byproduct. During the synthetic media era, it will be necessary to build trust perpetually through constant transparency, pre-crisis "trust-banking," and quick, assertive communication whenever misinformation is sent out. This indicates that today's crisis communication is not merely a matter of damage control but rather a process of building a complex system of credibility that can endure technologically advanced attacks.

The research, thus, points out the theoretical aspect and practical direction for the organizations dealing with a future where deepfake technology will be more prevalent and more persuasive. Those companies that make the effort and take the time to communicate, authenticate their products and services, and show the presence of top management will enjoy the advantage of the trust of the investors, the safety of their reputational capital, and less impact of the market fluctuations. The deepfake technology will make it harder to communicate during the crisis; thus, the imposition is clear: Trust through fast, transparent, and convincing communication will very soon be one of the main determinants of how well organizations cope with such crises in the digital age.

References:

Chesney, R., & Citron, D. (2019). *Deep fakes: A looming challenge for privacy, democracy, and national security*.
California Law Review, 107(6), 1753–1819 https://papers.ssrn.com/sol3/papers.cfmabstract_id=3213954
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. (2014). *Ongoing crisis communication: Planning, managing, and responding* (4th ed.). Thousand
Oaks, CA: SAGE Publications.
Hong, B., & Kim, D. (2019). *Investor trust and the effectiveness of corporate disclosure during crises*. *Journal of*
Financial Economics, 132(2), 265–286. https://doi.org/10.1016/j.jfineco.2018.11.005
Jiang, J. X., Petroni, K. R., & Wang, Y. (2010). *CEO incentives and earnings management: Evidence from earnings*
restatements. *Journal of Accounting and Economics, 49*(1-2), 105–120. https://doi.org/10.1016/j.jacceco.2009.09.006
Regan, H. (2024, February 4). *Deepfake scam tricks a multinational firm's employee into paying out $25 million*.
CNN. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk
Vaccari, C., & Chadwick, A. (2020). *Deepfakes and disinformation: Exploring the impact of synthetic political video*
on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1), 1–13. https://doi.org/10.1177/2056305120903408
Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence:
Introducing the business privacy calculus. *Journal of Business Research*, *142*, 1145–1156. https://www.sciencedirect.com/science/article/pii/S0148296324005149
Wagner, B., & Chen, L. (2025). AI-deepfake scams and the importance of a holistic communication security strategy. *Journal of Cybersecurity*, *6*, 53–61. https://link.springer.com/article/10.1365/s43439-025-00143-7
Manhattan Strategies. (2025). *Deepfake & misinformation rapid response framework for enterprise communications teams*. https://www.manhattanstrategies.com/insights/deepfake-misinformation-rapid-response-playbook
Porter, K. (2025). Tech PR trends: Navigating the digital frontier with innovation and strategy. *Agility PR*
Solutions. https://www.agilitypr.com/pr-news/branding-reputation/tech-pr-trends-navigating-the-digital-frontier-with-innovation-and-strategy
Sarkar, D. (2025). AI-generated misinformation and crisis management in corporate communications.
Forbes Communications Council. https://www.forbes.com/councils/forbescommunicationscouncil/2025/05/07/ai-generated-misinformation-and-crisis-management-in-corporate-communications/
Sidley Austin LLP. (2025, February). *Artificial Intelligence: U.S. financial regulator guidelines for responsible use*. Sidley. https://www.sidley.com/en/insights/newsupdates/2025/02/artificial-intelligence-us-financial-regulator-guidelines-for-responsible-use

The Guardian. (2024, May 10). *CEO of world's biggest ad firm targeted by deepfake scam*. *https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam*

MIT Sloan Review. (2024). *How Ferrari hit the brakes on a deepfake CEO*. *https://sloanreview.mit.edu/article/how-ferrari-hit-the-brakes-on-a-deepfake-ceo/*

Schwartz, C. (2025). 4 steps to tackle the risk of deepfake technology: Preparing PR strategies against synthetic media. *Agility PR Solutions*. https://www.agilitypr.com/pr-news/pr-tech-ai/4-steps-to-tackle-the-risk-of-deepfake-technology-preparing-pr-strategies-against-synthetic-media/

Rojas, K. (2022). How proactive communication wins over reactive. *Forbes Communications Council*.
https://www.forbes.com/councils/forbescommunicationscouncil/2022/05/17/how-proactive-communication-wins-over-reactive/

European Commission. (2025). *Digital Operational Resilience Act (DORA): Final regulatory technical*
standards. *https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en*

Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding* (4th ed.).
Sage Publications.
https://archive.org/details/ongoingcrisiscom0000coom_i9f6/page/n5/mode/1up

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1), 1–13.
https://doi.org/10.1177/2056305120903408

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national
security. *California Law Review, 107*(6), 1753–1820.
https://doi.org/10.2139/ssrn.3213954

West, D. M. (2019). *The future of work: Robots, AI, and automation*. Brookings Institution Press.
https://www.brookings.edu/books/the-automated-society/

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods*
approaches (5th ed.). Sage Publications.

Liu, B. F., Austin, L., & Jin, Y. (2011). How publics respond to crisis communication strategies: The interplay of information form and source. *Public Relations Review, 37*(4), 345–353.
https://doi.org/10.1016/j.pubrev.2011.08.004

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. 2003 Midwest Research-to-Practice Conference in Adult, Continuing, and *Community Education* (pp. 82–88). Purdue University.
https://scholarworks.indianapolis.iu.edu/bitstreams/976cec6a-914f-4e49-84b2-f658d5b26ff9/download

Kang, E., & Hwang, H.-J. (2023). The importance of anonymity and confidentiality for conducting survey research. *Journal of Research Practice & Ethics*, *4*(1). https://doi.org/10.15722/jrpe.4.1.202303.1

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing,*
62(1), 107–115.
https://doi.org/10.1111/j.1365-2648.2007.04569.x

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the
trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13.
https://doi.org/10.1177/160940691773384730

https://link.springer.com/article/10.1057/s41270-024-00353-8
https://www.sciencedirect.com/science/article/abs/pii/S0007681320300987

Appendix

1.1 Core Research Questions

1. To what extent does an immediate public denial by a tech company influence investor trust after a deepfake video
falsely shows the CEO announcing inflated earnings?
2. How do investors perceive the credibility and transparency of a company's leadership when the company issues a
delayed response to a deepfake misinformation event?
3. What communication factors such as timing, message tone, and clarity, do investors identify as most effective in
restoring trust after viewing a simulated deepfake crisis scenario involving a tech CEO?
4. How does prior exposure to deepfake technology affect investor susceptibility to misinformation and their
evaluation of a company's crisis response strategy?

1.2 Definition of Terms

Deepfake:
AI-generated synthetic media that realistically replicates a person's likeness (voice, face, or mannerisms), often used
to fabricate false video or audio content. In the context of this study, deepfakes refer to fraudulent CEO videos
announcing false financial information (Chesney & Citron, 2019).
Crisis Communication:

A strategic field within public relations focused on managing the dissemination of information during disruptive or

harmful events that threaten an organization's reputation, credibility, or operations (Coombs, 2014).

Proactive Communication Strategy:

A crisis response approach in which a company promptly addresses an issue—such as a deepfake incident—through

immediate denial or clarification, typically before a situation escalates further or misinformation spreads.

Reactive Communication Strategy:

A delayed response to a crisis event in which the organization issues a statement only after further verification,

internal review, or media attention. This approach may allow for accuracy but risks diminished trust due to perceived

hesitation.

Investor Trust:

The level of confidence investors place in a company's leadership, communication transparency, and decision-making

integrity—particularly in times of crisis or uncertainty (Hong & Kim, 2019).

Situational Crisis Communication Theory (SCCT):

A theory developed by W. Timothy Coombs that outlines how an organization should respond to crises based on the

level of responsibility it holds and the reputational threat posed. SCCT emphasizes the importance of response

timing, clarity, and message consistency (Coombs, 2007).

Synthetic Media:

Digitally manipulated or fully AI-generated media content designed to imitate real information or communication.Deepfakes are a specific type of synthetic media.

Appendix A

Table 1.1 Critical Knowledge voids

Gap	Consequence	Research Priority
Cross-cultural responses	Non-Western firms use 43% more authoritarian messaging	High
Investor segmentation	Retail investors 3x more likely to panic-sell vs. institutions	Critical
Simulation realism	78% of drills use primitive deepfakes	Medium

Table 1.2 Defense Effectiveness Matrix

Defense Layer	Ferrari	WPP	Hong Kong
Technical (AI detection)	❌	❌	❌
Procedural (2FA)	✓	❌	❌
Cultural/Social	✓	✓	❌

Appendix B

Table 2.1 Timing of response

Code	Category	Description
T1	Proactive (<2 hrs)	Company issued a public statement or action within 2 hours of viral spread
T2	Semi-Proactive	Company responded between 2–6 hours
T3	Reactive (>6 hrs)	Response occurred after 6+ hours of widespread attention

T4	No Timed Response	Response not clearly timestamped or delayed by >24 hours

Table 2.2 Tone of Response

Code	Category	Description
To1	Defensive	Denies fault, shifts blame, or focuses on discrediting the video
To2	Reassuring	Calms stakeholders, expresses control, affirms integrity
To3	Transparent	Fact-based, confident, avoids emotional manipulation
To4	Ambiguous	Vague, unclear, or inconsistent in language or positioning
To5	Absent Tone	No tone discernible—press release only or robotic statement

Table 2.3 Transparency Level

Code	Category	Description
Tr1	High	Includes technical evidence (e.g., cybersecurity audit, video forensics)
Tr2	Moderate	Acknowledges deepfake but provides minimal technical proof
Tr3	Low	Asserts position but offers no details or only references third parties
Tr4	Misleading	Offers contradictory or unverifiable statements

Table 2.4 Platforms used

Code	*Platform*	*Description*
P1	*Corporate Website*	*Official IR or newsroom page, SEC filings*
P2	*Social Media*	*CEO/company posts on Twitter, LinkedIn, etc.*
P3	*Video Statement*	*CEO/Executive records a direct-to-camera statement (e.g., YouTube, Zoom)*
P4	*News Media*	*Interviews, press conference, or media appearance*
P5	*Third-Party Platform*	*Via fact-checkers (e.g., Snopes, NewsGuard) or cybersecurity firms*

Table 2.5 SCCT crisis response

Code	Strategy Type	SCCT Description
S1	Denial	Denies deepfake event or its relevance entirely
S2	Diminish	Acknowledges but downplays damage or intent
S3	Rebuild	Accepts incident occurred, seeks to rebuild trust (e.g., legal action, audits)
S4	Bolster	Highlights company's strong record, ethics, or past actions
S5	Mixed	Combination of above; e.g., denial + bolster or diminish + rebuild

Table 2.6 Stakeholder-Focused Messaging

Code	Category	Description
M1	Yes – Investors	Directly references shareholder/investor concerns or market impact
M2	General Public	Targets general public or customers
M3	Regulatory Focus	Targets SEC, legal action, compliance messaging
M4	None/Unclear	Audience not clearly defined

Appendix C

3.1 Codebook

Variable	code	description
Timing	T1,T2,T3,T4	T1= Proactive(<2 hrs),T2=Semi-proactive(2-6 hrs),T3= Reactive (>6 hrs), T4= No response(>24 hrs)
Tone	To1,To2,To3,To4,To5	To1= Defensive, To2= Reassuring, To3= Transparent, To4= Ambiguous, To5= Absent
Transparency	Tr1,Tr2,Tr3,Tr4	Tr1= High, Tr2= Moderate, Tr3= Low, Tr4= Misleading
Platform	P1,P2,P3,P4,P5	P1= Corporate website, P2= Social Media, P3= Video statement, P4= News media, P5= Third-party
SCCT	S1,S2,S3,S4,S5	S1=Denial,S2= Diminish, S3=Rebuild, S4= Bolster, S5= Mixed
Stakeholder	M1,M2,M3,M4	M1=Yes, M2= General public, M3= Regulatory focus, M4= None

3.2 Coding Matrix

Case ID	Case Name	Year	Timing (T)	Tone (TO)	Transparency	Platfroms (P)	SCCT (S)	Stakeholder (	Notes
C1	UK energy firm	2019	T3	To5	Tr4	P5	S1	M4	No official statement,misleading third-party reports
C2	Ferrari	2024	T1	To3	Tr1	P1,P2	S3	M1	Proactive verification and press releases within hours; investor reassurance on linkedin
C3	WPP	2024	T2	To4	Tr2	P1,P2,P4	S5	M2	Mixed response with factual tone, rapid containment reported in news media
C4	Hong kong finance	2024	T3	To1	Tr3	P1,P4	S2	M3	Defensive reactive response,limited transparency aimed at regulators

Table 3.3 Reliability Analysis (Cronbach's Alpha)

Construct	Items	Cronbach's α	Interpretation
Investor Trust	3	0.937	Excellent internal consistency
Transparency & Credibillity	4	0.949	Excellent internal consistency
Investment Intention	3	0.831	Good internal consistency

Table 3.4 Descriptive statistics

Construct	Group	N	Mean (M)	Standard Deviation (SD)
Investor Trust	Proactive	13	3.77	1.16
	Reactive	17	3.08	1.13
Transparency & Credibility	Proactive	13	3.75	1.13
	Reactive	17	3.09	0.96

Construct	Group	N	Mean (M)	Standard Deviation (SD)
Investment Intention	Proactive	13	3.69	1.21
	Reactive	17	2.90	0.93
Emotional Response	Proactive	13	3.38	1.16
	Reactive	17	2.76	0.64

Table 3.5 Trust Independent t-test

T-Test

Group Statistics

	Proactive vs reactive numeric	N	Mean	Std. Deviation	Std. Error Mean
Trust_mean	1.00	13	3.7692	1.15778	.32111
	2.00	17	3.0784	1.12749	.27346

Independent Samples Test

		t-test for Equality of Means			
				Significance	
		t	df	One-Sided p	Two-Sided p
Trust_mean	Equal variances assumed	1.644	28	.056	.111
	Equal variances not assumed	1.638	25.613	.057	.114

Independent Samples Test

		t-test for Equality of Means		
				95% Confidence Interval of the ...
		Mean Difference	Std. Error Difference	Lower
Trust_mean	Equal variances assumed	.69080	.42023	-.17000
	Equal variances not assumed	.69080	.42177	-.17680

Independent Samples Test

		t-test for Equality ..	
		95% Confidence Interval of the ...	
		Upper	
Trust_mean	Equal variances assumed	1.55160	
	Equal variances not assumed	1.55840	

Table 3.6 Transparency Independent t-test

T-Test

Group Statistics

	Proactive vs reactive numeric	N	Mean	Std. Deviation	Std. Error Me
Transparency_mean	1.00	13	3.7500	1.12731	.3126
	2.00	17	3.0882	.96396	.2338

Independent Samples Test

		t-test for Equality of Means			
				Significance	
		t	df	One-Sided p	Two-Sided p
Transparency_mean	Equal variances assumed	1.732	28	.047	.094
	Equal variances not assumed	1.695	23.630	.052	.103

Independent Samples Test

		t-test for Equality of Means		
				95% Confidence Interval of the ...
		Mean Difference	Std. Error Difference	Lower
Transparency_mean	Equal variances assumed	.66176	.38212	-.12097
	Equal variances not assumed	.66176	.39041	-.14466

Independent Samples Test

		t-test for Equality ..
		95% Confidence Interval of the ...
		Upper
Transparency_mean	Equal variances assumed	1.44450
	Equal variances not assumed	1.46819

Table 3.7 Investment Independent t-test

T-Test

Group Statistics

	Proactive vs reactive numeric	N	Mean	Std. Deviation	Std. Error Mean
Investment_mean	1.00	13	3.6923	1.21306	.33644
	2.00	17	2.9020	.92620	.22464

Independent Samples Test

		t-test for Equality of Means			
				Significance	
		t	df	One-Sided p	Two-Sided p
Investment_mean	Equal variances assumed	2.026	28	.026	.052
	Equal variances not assumed	1.954	21.830	.032	.064

Independent Samples Test

		t-test for Equality of Means		
				95% Confidence Interval of the ...
		Mean Difference	Std. Error Difference	Lower
Investment_mean	Equal variances assumed	.79035	.39006	-.00866
	Equal variances not assumed	.79035	.40454	-.04900

Independent Samples Test

		t-test for Equality ..
		95% Confidence Interval of the ...
		Upper
Investment_mean	Equal variances assumed	1.58936
	Equal variances not assumed	1.62969

Independent Samples Effect Sizes

				95% Confidence Interval	
		Standardizer[a]	Point Estimate	Lower	Upper
Investment_mean	Cohen's d	1.05870	.747	-.008	1.488
	Hedges' correction	1.08815	.726	-.007	1.448
	Glass's delta	.92620	.853	.063	1.621

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Table 3.8 Emotional Independent t-test

T-Test

Group Statistics

	Proactive vs reactive numeric	N	Mean	Std. Deviation	Std. Error Mean
emotional_mean	1.00	13	3.3846	1.15747	.32103
	2.00	17	2.7647	.64026	.15528

Independent Samples Test

		t-test for Equality of Means			
				Significance	
		t	df	One-Sided p	Two-Sided p
emotional_mean	Equal variances assumed	1.871	28	.036	.072
	Equal variances not assumed	1.738	17.552	.050	.100

Independent Samples Test

		t-test for Equality of Means		
				95% Confidence Interval of the ...
		Mean Difference	Std. Error Difference	Lower
emotional_mean	Equal variances assumed	.61991	.33127	-.05867
	Equal variances not assumed	.61991	.35661	-.13067

Independent Samples Test

		t-test for Equality ..	
		95% Confidence Interval of the ...	
		Upper	
emotional_mean	Equal variances assumed	1.29849	
	Equal variances not assumed	1.37049	

Independent Samples Effect Sizes

				95% Confidence Interval	
		Standardizer[a]	Point Estimate	Lower	Upper
emotional_mean	Cohen's d	.89912	.689	-.060	1.428
	Hedges' correction	.92414	.671	-.059	1.389
	Glass's delta	.64026	.968	.161	1.751

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

3.9 Summary of independent t-tests

Construct	t(df)	p(two-tailed)	Mean Difference	Cohen's d
Investor Trust	t(28)= 1.64	0.111	0.69	0.61
Transparency & Credibility	t(28)= 0.94	0.94	0.66	0.64
Investment Intention	t(28)= 2.03	0.052	0.79	0.75
Emotional Response	t(28)= 1.87	0.072	0.62	0.69