Journal of Risk Analysis and Crisis Response, 2025, 15(2), 239-272
https://jracr.com/
ISSN Print: 2210-8491
ISSN Online: 2210-8505

Article

Effective Communication as A Pillar of Cybersecurity: Managing Incidents and Crises in the Digital Era

Jersain Zadamig Llamas Covarrubias [1,*]

[1] Division of Legal Studies, University Center of Social Sciences and Humanities, University of Guadalajara, Guadalajara (44100), Jalisco, Mexico
* Correspondence: jersain.llamas@academicos.udg.mx

Received: January 6, 2025; Received in revised form: March 10, 2025; Accepted: April 26, 2025; Available online: June 30, 2025

Abstract: Effective communication is a critical yet often overlooked component of cybersecurity incident response and crisis management. While existing frameworks, such as ISO/IEC 27035 and NIST SP 800-61, focus on technical measures, they provide limited guidance on structured communication strategies that enhance resilience, mitigate reputational risks, and ensure regulatory compliance. This research addresses this gap by examining the role of strategic communication in cybersecurity through a qualitative, descriptive-analytical approach. Drawing from international standards, regulatory frameworks (e.g., GDPR, DORA, CIRCIA), and comparative case studies, including the CrowdStrike Outage and Equifax Breach, this research identifies best practices and common pitfalls in cyber crisis communication. Analysis highlight that timely disclosure, message consistency, and proactive stakeholder engagement are essential for effective incident management. The investigation proposes a Unified Communication Model that integrates structured communication protocols into cybersecurity incident response frameworks, enhancing organizational resilience. The analytical insights have significant implications for policy and practice, emphasizing the need for regulatory harmonization and proactive disclosure policies. By embedding communication strategies within cybersecurity frameworks, organizations can improve crisis management outcomes, maintain stakeholder trust, and navigate an evolving cyber threat landscape.

Keywords: Cybersecurity; Crisis Communication; Incident Response; Cyber Threats; Regulatory Compliance; Strategic Messaging; Stakeholder Engagement

1. Introduction

Cybersecurity incident management has traditionally prioritized technical measures, while often overlooking an equally critical element: structured communication. Structured communication refers to intentional, pre-defined, and adaptive processes that guide messaging during cybersecurity incidents, ensuring information is disseminated clearly and consistently. Recent high-profile cases illustrate this point: the proactive, transparent strategy during the CrowdStrike Outage maintained stakeholder trust and facilitated efficient recovery, while fragmented messaging in the Costa Rica Ransomware Attack exacerbated uncertainty and prolonged disruption. Similarly, the Equifax Breach and Uber Hack demonstrate how delayed or misleading disclosures trigger severe reputational damage and financial penalties. These cases underscore that cybersecurity incidents are

multidimensional challenges that demand strategic communication practices. Specifically, practices such as timely and accurate information dissemination, audience-specific messaging, and maintaining an appropriate tone are essential. Moreover, established communication protocols, like incident response communication frameworks and crisis management guidelines, are vital for managing stakeholder expectations, meeting regulatory requirements, and shaping public perception.

Despite its importance, the integration of communication strategies into cybersecurity frameworks remains underexplored. Regulatory standards such as ISO/IEC 27035, NIST SP 800-61, GDPR, DORA, and CIRCIA provide guidance on incident reporting but offer limited direction on designing communication strategies for different audiences and scenarios. Current models focus primarily on technical containment and compliance but inadequately address how communication timing, message consistency, audience segmentation, and transparency influence crisis outcomes. Consequently, organizations often adopt ad hoc communication strategies, leading to inconsistent messaging and loss of stakeholder confidence.

Cybersecurity incidents present a complex interplay between various factors: different threat types, diverse audiences (technical teams, executives, regulators, customers, media), and multiple communication modes. This research addresses this gap by examining the role of structured communication in cybersecurity incident management through three key dimensions: timeliness, content clarity, and audience adaptation. Timeliness is critical, as early disclosure fosters trust, whereas delays amplify risks. Content clarity involves balancing technical accuracy, legal considerations, and public reassurance. Audience adaptation acknowledges that diverse stakeholder groups require tailored messaging to avoid misinterpretation or panic.

By conducting a qualitative, descriptive-analytical investigation that integrates insights from international standards, regulatory frameworks, and comparative case studies, this research aims to: 1. identify key components of effective communication in cyber incident management; 2. evaluate how existing frameworks can be adapted to embed these protocols; and 3. propose actionable recommendations for optimizing crisis communication. Through this approach, the work contributes to bridging the gap between technical cybersecurity response and effective crisis communication, offering both theoretical advancements and practical recommendations for enhancing cyber resilience in an increasingly complex digital landscape.

2. Methodology

This research employs a qualitative, descriptive-analytical approach to examine the integration of strategic communication protocols within cybersecurity incident management and crisis response frameworks. Given the complexity and contextual nature of cybersecurity communication, a qualitative methodology allows for an in-depth exploration of patterns, challenges, and best practices that may not be fully captured through purely quantitative means. The research design integrates three core components: 1. an extensive review of literature and regulatory frameworks; 2. an empirical case analysis; and 3. a structured thematic analysis to identify recurring communication strategies and challenges across different cybersecurity incidents.

2.1. Research Design

The research follows an exploratory-descriptive design, aiming to analyze how organizations implement communication strategies during cybersecurity incidents. This design is appropriate given the evolving nature of cyber threats and the necessity of examining communication as a strategic element beyond technical security measures. The research questions guiding this investigation include:

1) What are the key components of an effective cybersecurity incident communication strategy, and how do they align with international standards and regulatory frameworks?

2) How do international standards and regulatory framework's structure cybersecurity communication?

3) What lessons can be drawn from high-profile cybersecurity incidents regarding the timing, transparency, and consistency of communication?

To answer these questions, the investigation combines document analysis and research based on cases, offering a holistic view of communication strategies across regulatory frameworks and real-world cybersecurity incidents.

2.2. Data Collection

The research relies on two primary data sources:

1) Documentary Analysis: This includes a systematic review of international standards (e.g., ISO/IEC 27035, NIST SP 800-61, ISO 22361), regulatory mandates (GDPR, DORA), and peer-reviewed literature on cybersecurity incident response and crisis communication. This documentary analysis provides a theoretical and regulatory foundation for evaluating communication practices in cybersecurity.

2) Research based on cases: A purposive sampling approach was used to select high-profile cybersecurity incidents that exemplify both best practices and communication failures. The selected cases include:

a) CrowdStrike Outage - Example of proactive and transparent communication.
b) Costa Rica Ransomware Attack - Illustrates fragmented crisis communication.
c) WannaCry - Highlights challenges in global cyber incident coordination.
d) Sony Pictures Hack - Demonstrates internal communication failures.
e) Uber Hack – Example of reputational risks from delayed disclosure.
f) Target Hack - Case of financial and reputational damage from miscommunication.
g) MITRE Breach - Best practices in transparency and post-incident response.
h) Equifax Breach - Example of poor crisis communication and public backlash.

Each case was examined through publicly available reports, corporate disclosures, regulatory filings, and academic analyses. The inclusion criteria were:

1) The incident had a significant impact on public perception, regulatory response, or financial stability.

2) Publicly available information allowed for a structured analysis of communication strategies.

3) The case provided insights into best practices or common pitfalls in cybersecurity communication.

2.3. Data Analysis

A structured thematic analysis was conducted using iterative coding to identify patterns in cybersecurity communication across case studies and regulatory frameworks. The analysis followed these steps:

1) Preliminary Coding: Key communication elements were identified from literature, standards, and cases (e.g., incident notification timing, message framing, stakeholder coordination).

2) Categorization: Themes were grouped into broader categories aligned with established incident response and crisis management models, including:

a) Timeliness and transparency in incident disclosure.

b) Internal coordination among cybersecurity, legal, and public relations teams.

c) Stakeholder engagement (e.g., regulators, customers, media).

d) Regulatory compliance with disclosure mandates.

e) Crisis escalation and message consistency across communication channels.

3) Triangulation: Analysis from case studies were cross-referenced with industry best practices (e.g., ISO/IEC 27035, NIST SP 800-61). This ensured that conclusions were supported by multiple independent sources.

4) Comparative Analysis: Case studies were compared to identify key differentiators between effective and ineffective cybersecurity communication strategies.

2.4. Reliability and Validity

To enhance research rigor, the investigation employed:

1) Triangulation of data sources, integrating regulatory documents, case studies, and literature.

2) Inter-coder reliability, ensuring consistency in thematic coding through structured coding guidelines and consensus discussions.

3) Cross-verification with industry standards and regulatory mandates to validate the relevance of observations.

2.5. Limitations and Future Research

This research is qualitative and focuses on case studies, which may limit the generalizability of conclusions across all industries and organizations. Additionally, it does not incorporate a quantitative component (e.g., surveys or frequency analysis of communication responses), which could provide statistical validation of observed patterns. Future research could:

1) Employ mixed-methods approaches, incorporating empirical surveys or experiments to measure the effectiveness of different communication strategies.

2) Conduct cross-industry comparative studies to examine variations in cybersecurity communication across sectors.

3) Explore the role of AI-driven communication tools in automating cybersecurity crisis messaging.

3. Literature Review

Effective communication has emerged as a cornerstone in the management of cybersecurity incidents and crises. Over the past decade, researchers have developed multifaceted frameworks and models that address both the proactive and reactive dimensions of crisis communication. This review

synthesizes key contributions from the literature, highlighting theoretical frameworks, sector-specific strategies, and the role of social and technological factors in enhancing organizational resilience.

3.1. Frameworks for Cyber Crisis Communication

Several studies propose structured models that delineate clear phases for managing cybersecurity incidents. Knight and Nurse introduce an empirically grounded framework for corporate communication following data breaches. Their model emphasizes a two-phase approach, starting with pre-crisis planning (establishing communication aims, rehearsals, and stakeholder coordination) and transitioning into a crisis response phase that focuses on timely disclosures, strategic message framing, and regulatory compliance [1]. Complementarily, Manley and McIntire provide a comprehensive guide that argues for embedding robust communication strategies within incident management. Their work stresses that proactive planning, defining roles, tailoring messages to diverse audiences, and aligning with standards such as the NIST Cybersecurity Framework, is vital for mitigating reputational damage and ensuring swift crisis resolution [2].

In the context of public institutions, Østby and Katt propose the Cyber Incident Handling Role Model (CIHRM) for municipal environments. Their role-based approach integrates traditional crisis management with cyber-specific functions, thereby ensuring that experts, from CERTs to SOC teams, are strategically aligned during both the response and recovery phases [3]. Reinforcing the need for cohesive strategies, Reinhold et al. call for convergence in risk and crisis communication research [4]. Their analysis reveals that disciplinary silos have long hindered the development of universal frameworks, thereby advocating for interdisciplinary approaches that bridge insights from natural hazards, public health, and cybersecurity.

3.2. Cross-Industry and Comparative Perspectives

Insights drawn from diverse industries provide valuable lessons for cybersecurity crisis communication. A comparative analysis across healthcare, finance, and technology reveals that while core principles, such as timeliness, transparency, and empathy, are universal, their operationalization must be industry-specific [5]. For example, Ruohonena et al. demonstrate that data breach incidents require immediate self-disclosure, accountability, and adherence to regulations like GDPR and the NIS2 directive to maintain public trust [6]. Furthermore, conceptualizing cyber crises as transboundary events, Backman compares incidents such as the Estonia 2007 attack and the UK 2017 ransomware case, emphasizing the need for collaborative, adaptive strategies that transcend traditional jurisdictional boundaries [7].

The importance of bridging communication gaps is further underscored by Bolton, who identifies significant disconnects between cybersecurity and emergency management professionals due to specialized jargon [8]. His recommendations for a common language and cross-sector training are echoed in Mott, Nurse, and Baker-Beall's exploration of lessons learned from the SARS-CoV-2 pandemic [9]. They argue that cross-stakeholder engagement and preemptive, transparent messaging, practices honed during public health crises, can be effectively transferred to the realm of cybersecurity.

3.3. National and Organizational Strategies

At the national and organizational levels, coordinated communication emerges as a critical success factor. Ramadhianto et al. analyze Indonesia's strategic response through Presidential Regulation No. 47, which emphasizes systematic communication among state agencies and cybersecurity organizations to facilitate inter-agency coordination [10]. In parallel, Groșu et al. propose the "5C Structured Approach to Critical Communication," a phased model that encompasses crisis understanding, coordination, collaboration for validation, clear messaging, and feedback loops, underscoring the emerging role of AI-driven tools in enhancing these processes [11]. Complementary studies on corporate crisis management reveal alarming gaps in preparedness; a data-driven analysis shows that many organizations lack dedicated crisis management plans and resources, highlighting the transformative potential of structured communication strategies for reducing both reputational and financial risks [12].

3.4. National and Organizational Strategies

A growing body of work focuses on the importance of integrating multi-phase approaches to build digital resilience. Mahmood et al. propose a digital resilience framework tailored to the Higher Education and Research Sector, outlining distinct phases from pre-crisis planning and crisis absorption to adaptation and post-crisis evaluation [13]. Similarly, Moerschell and Novak emphasize the need for "alignment" in university settings, where consistent messaging across pre-crisis, crisis, and post-crisis stages is crucial to prevent misinformation and operational disruptions [14]. Broadening the scope, Steen et al. introduce a framework that rethinks traditional business continuity management by integrating resilience engineering principles with anticipated improvisation, a concept that reinforces the importance of flexible, real-time communication protocols [15]. Kiiveri et al. further illustrate this point through a mobile-based crisis management model for SMEs, demonstrating how embedded communication features in a dedicated application can enhance situational awareness and enable coordinated responses [16].

3.5. National and Organizational Strategies

Understanding the human and social dimensions of crisis communication is essential for tailoring messages to diverse audiences. Liu et al. highlight that media communication significantly influences the reception of risk information in community settings, suggesting that message design must consider demographic factors such as age and education. Insights from other high-stakes crises are equally instructive [17]. Yang et al. analyze crisis communication during nuclear accidents, showing how public panic can be mitigated through clear, transparent messaging that bridges technical and lay language [18]. In a similar vein, Sparf and Öhman discuss how social capital shapes risk perception and the effectiveness of digital communication channels, particularly for marginalized groups [19].

Strategic communication at the national level also plays a critical role in countering hybrid threats. An article on information security communications highlights Ukraine's and the European Union's efforts to combat disinformation through integrated communication strategies that combine public narratives, media literacy, and coordinated messaging [20]. Looking ahead, a futures-oriented analysis employing a PESTLE framework identifies 153 potential crisis phenomena, thereby stressing the need for proactive, holistic crisis management strategies that incorporate adaptive communication [21]. Moreover, Borden et al. demonstrate that linguistic abstraction in social media

language can serve as an indicator of crisis attribution, suggesting that monitoring language use can provide early warnings of escalating blame [22]. Zhan and Zhao further explore this relational perspective by showing how negative emotions amplify adverse stakeholder responses, and how efficacy-enhancing communication can mitigate these effects [23].

Finally, the digital landscape itself is a battleground for narratives. Moral documents how the European Union's digital diplomacy on Twitter during the COVID-19 crisis evolved from fragmented to coherent messaging, ultimately restoring public trust [24]. In contrast, Manfredi, Amado, and Gómez-Iniesta caution that state-sponsored disinformation campaigns deliberately exploit emotional narratives to undermine institutional credibility [25]. Their discoveries underscore the need for crisis communication strategies that not only disseminate accurate information but also actively counteract emotionally charged misinformation.

In conclusion, the reviewed literature converges on the central tenet that structured, adaptive communication is indispensable for effective incident response and crisis management in the digital era. From empirically grounded frameworks and cross-industry analyses to insights into social and psychological factors, these studies collectively demonstrate that proactive planning, role clarity, and the strategic use of technology and media are key to safeguarding reputation and fostering resilience. This comprehensive synthesis not only informs current best practices but also paves the way for future research aimed at integrating multidisciplinary perspectives into a unified approach for cybersecurity crisis communication.

4. Problems and Possible Solutions

As cybersecurity continues to evolve in response to increasingly complex threats, the role of communication has become foundational to both defensive and proactive security measures. The intersection between communication and cybersecurity is multifaceted, encompassing the protection of communication as a vital asset, a medium for secure information exchange, and a strategic tool to achieve broader cybersecurity objectives. By examining communication through these lenses, we can better understand how targeted communication strategies contribute to an organization's resilience and stability. This section explores these dimensions in depth, emphasizing how safeguarding communication infrastructure, ensuring secure transmission channels, and employing effective communication techniques support organizations in both preventing and responding to cyber incidents.

The primary intersection between communication and cybersecurity encompasses safeguarding communication as a critical asset, a medium, and a goal. When regarded as a critical asset, communication involves protecting infrastructure integral to organizational stability and resilience. In the United States, the Communications Sector is designated as critical infrastructure, as outlined in the National Infrastructure Protection Plan (NIPP) 2013. This plan meets the requirements of Presidential Policy Directive (PPD) 21 by integrating risk management strategies across critical infrastructure [26]. This designation reflects the sector's essential role in maintaining national security, economic stability, and public safety through its interconnections with other critical sectors, such as energy, transportation, and emergency services. Similarly, in the European Union, communications infrastructure is considered critical under Directive (EU) 2022/2557 on the resilience of critical entities, alongside the NIS 2 Directive (EU) 2022/2555, which emphasizes the importance of securing public electronic communication networks and services to ensure societal stability [27,28]. These frameworks

demonstrate a transatlantic commitment to fortifying communication infrastructures against disruptions, underscoring their role in sustaining interconnected sectors and promoting national resilience.

As a medium, communication in cybersecurity focuses on protecting the transmission of information, extending beyond mere data content to ensure the integrity and confidentiality of the communication process itself. Network security, requires safeguarding communication channels against a variety of attacks that can intercept, alter, or disrupt data flows. These threats include active attacks, such as spoofing, and denial-of-service, which compromise network integrity by altering communication routes or overwhelming system resources. In contrast, passive attacks, such as eavesdropping and traffic analysis, aim to capture data in transit without altering it [29]. To mitigate these vulnerabilities, encryption and monitoring tools play a critical role in securing network channels from malicious entities attempting unauthorized access [29].

Approaching communication as a goal in cybersecurity highlights several critical aspects where effective, targeted communication fosters mutual understanding and support among distinct audiences:

- Communication with Leadership: The Chief Information Security Officer (CISO) is responsible for bridging the gap between technical cybersecurity insights and board-level decision-making. By effectively communicating risks and resource needs, the CISO helps secure the necessary budget and support for cybersecurity initiatives [30].
- Cybersecurity Awareness Program: An effective cybersecurity awareness (CSA) program prioritizes clear communication to influence knowledge, attitudes, and behaviors organization-wide [31].
- Cybersecurity Tabletop Exercises: Effective communication is crucial in cybersecurity, and tabletop exercises provide a structured approach to enhancing incident response readiness. By simulating incidents, these exercises help organizations clarify roles, improve collaboration, and reduce response times, ultimately minimizing breach [32].
- Communication within Cybercriminal Platforms: Social networks on the Deep and Dark Web serve as critical spaces for cybercriminals to exchange knowledge, sell illicit materials (e.g., breached data), and coordinate activities. Researchers studying these forums can gain insights into cybercriminal behavior, enabling proactive threat intelligence that informs security strategies to mitigate emerging threats [33].
- Communication in Threat Intelligence: Standards such as STIX and MISP facilitate information exchange, informing organizations about tactics, techniques, and procedures used by malicious actors, thus strengthening defenses [34].
- Regulatory Requirements for Incident Notification: Certain regulatory frameworks, including the General Data Protection Regulation (GDPR) of 2016; and the U.S. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 [35], mandate timely incident notifications to stakeholders, emphasizing the importance of communication in promoting transparency and ensuring compliance. Additionally, the U.S. Securities and Exchange Commission (SEC) has introduced specific disclosure requirements for publicly traded companies regarding material cybersecurity incidents. As of July 26, 2023, the SEC mandates that companies disclose incidents deemed material under Item 1.05 of Form 8-K, requiring disclosure within four business days of determining the materiality of an incident [36].

- Responsible Disclosure Programs: Responsible disclosure is increasingly recognized as a critical component of cybersecurity communication, enabling the safe reporting of vulnerabilities to vendors or manufacturers:
  - In the European Union, the Cyber Resilience Act [37] proposes that manufacturers of products with digital elements implement coordinated vulnerability disclosure policies. This policy facilitates vulnerability reporting, enabling manufacturers to address vulnerabilities before public disclosure. The Act also encourages the use of bug bounty programs to incentivize individuals and entities to report vulnerabilities, helping prevent the sale of exploitable vulnerabilities on black markets.
  - In the United States, the Internet of Things Cybersecurity Improvement Act of 2020 requires the National Institute of Standards and Technology (NIST) to develop guidelines for vulnerability reporting and disclosure, particularly for federal agencies and IoT devices. Additionally, CISA's Binding Operational Directive 20-01 mandates that federal civilian agencies publish vulnerability disclosure policies, ensuring that vulnerability reporting processes are accessible and actionable [38].
- Strategic Communication for Incident Response and Crisis Management: Developing robust information security communication strategies is crucial for managing incidents and reducing risks from hybrid warfare and enemy attacks. Effective crisis communication relies on cooperative models among stakeholders, promoting rapid information sharing, decision-making, and coordinated responses. Expanding alliances enhances the impact of cybersecurity messaging, strengthening collective resilience. Importantly, strategic communication must be continuous and adaptable to evolving threats and diverse audience needs, ensuring resilient crisis response and reinforcing cybersecurity efforts [39].

In conclusion, this research article aims to present essential communication techniques and strategic approaches for incident response and effective crisis management. By focusing on a standardized framework, this research outlines concise, actionable steps that organizations can adopt to strengthen their crisis communication capabilities. These strategies empower companies to communicate transparently and decisively during cybersecurity incidents, fostering stakeholder resilience and trust. Ultimately, by integrating these practices, organizations can enhance their overall security posture and readiness, ensuring that they respond effectively to threats and build a foundation for continuous improvement and adaptation in an ever-evolving threat landscape.

5. Case Analysis: Best Practices and Pitfalls in Cybersecurity Communication

Effective communication plays a pivotal role in cybersecurity incident management and crisis response. Beyond the technical measures required to contain a cyber incident, organizations must strategically manage internal coordination, public messaging, and stakeholder engagement to mitigate reputational and operational risks. The absence of a well-structured communication framework often exacerbates crisis fallout, leading to regulatory scrutiny, erosion of public trust, and prolonged recovery periods.

This section employs a comparative case-based research approach to analyze major cybersecurity incidents, assessing how communication strategies influenced crisis outcomes. The analysis is structured around four critical dimensions, aligned with best practices from international cybersecurity frameworks:

- Timeliness of Disclosure: Speed and responsiveness in public communication.

- Message Consistency and Transparency: Coherence, accuracy, and clarity in messaging across all stakeholders.
- Stakeholder Engagement: Effectiveness in communicating with affected parties, regulators, and the public.
- Regulatory Compliance: Adherence to industry-specific disclosure requirements and cybersecurity regulations.

The following cases illustrate best practices and common pitfalls in cybersecurity crisis communication, providing insights into proactive strategies that organizations can adopt to strengthen resilience.

5.1. Case Studies in Cybersecurity Communication

5.1.1. Proactive and Transparent Communication: CrowdStrike Outage of 2024

In July 2024, a defective Falcon content update from CrowdStrike caused a global service outage, disrupting millions of endpoints, including critical infrastructure, financial institutions, and enterprises worldwide. Customers faced system crashes and operational paralysis, leading to severe economic disruptions in multiple sectors. Within minutes of detecting the issue, CrowdStrike issued a public statement acknowledging the incident, identifying the problematic update, and providing clear remediation steps. The company engaged continuously with affected customers, updating them in real time through official channels and collaborating with major technology partners, including Microsoft, to accelerate remediation [40].

- Best Practice: Proactive disclosure reduced uncertainty, demonstrating accountability and commitment to transparency.
- Key Lesson: Proactive disclosure and continuous updates foster stakeholder trust and minimize speculation.

5.1.2. Fragmented and Delayed Crisis Response: Costa Rica Ransomware Attack of 2022

In April 2022, the Conti ransomware group launched a coordinated cyberattack on Costa Rica's government, encrypting tax systems, customs platforms, healthcare databases, and financial services. The attack crippled public administration, forcing government agencies to shut down essential services. The initial response was fragmented and delayed. Government officials provided contradictory statements, creating uncertainty and panic among citizens and businesses. It took several days for authorities to declare a national emergency, and communication with the public remained sporadic and inconsistent [41].

- Pitfall: The absence of a pre-established crisis communication framework led to confusion and eroded public confidence in government institutions.
- Key Lesson: A structured communication plan is critical to ensure public trust and operational continuity during cyber crises.

5.1.3. Lack of Unified Messaging: WannaCry Ransomware Attack of 2017

The WannaCry ransomware attack of May 2017 exploited the EternalBlue vulnerability, affecting over 230,000 computers in 150 countries. The attack severely impacted hospitals, banks, telecom providers, and transportation networks, forcing some organizations to shut down operations

for days. Despite the rapid deployment of security patches, public communication was disorganized. Government agencies, cybersecurity firms, and affected companies failed to coordinate messaging, leading to inconsistent guidance on mitigation strategies. Many victims were left uncertain about whether to pay ransoms or how to restore systems [42].

- Pitfall: The lack of a coordinated communication response prolonged the impact of the attack.
- Key Lesson: Predefined incident communication protocols are necessary to ensure a unified, authoritative response.

5.1.4. Internal Communication Failures: Sony Pictures Hack of 2014

In November 2014, North Korean-linked hackers targeted Sony Pictures, stealing sensitive corporate data, unreleased films, and employee records. The attackers demanded the cancellation of a film release, issuing threats of retaliation. Sony's internal misalignment led to inconsistent external messaging. The company initially downplayed the breach, before later confirming massive data exfiltration. Furthermore, the consideration of a counterattack ("hack-back") raised legal and ethical concerns [43].

- Pitfall: Poor internal coordination resulted in contradictory public messaging, further escalating the crisis.
- Key Lesson: Organizations must establish internal crisis communication governance before engaging in external messaging.

5.1.5. Concealed Disclosure: Uber Hack of 2016

Uber suffered a data breach affecting 57 million users but deliberately concealed the incident by paying hackers $100,000 to delete the stolen data. The breach remained undisclosed for over a year. Uber violated breach notification laws, failing to notify users, regulators, or law enforcement in a timely manner. When the breach was finally disclosed, it led to legal penalties, executive resignations, and reputational damage [44].

- Pitfall: Concealment strategies increase legal and financial risks.
- Key Lesson: Transparency in breach disclosure is both a legal obligation and a reputational safeguard.

5.1.6. Impact of Delayed Disclosure: Target Hack of 2013

A massive data breach at Target compromised the personal and financial data of 40 million customers. Attackers gained access via a third-party HVAC contractor, infiltrating the company's payment processing systems. Target delayed notifying affected customers, allowing unauthorized transactions to escalate. The lack of clear communication with banks and financial institutions prolonged the incident's economic impact [45].

- Pitfall: Delayed disclosure increased consumer exposure to fraud and financial losses.
- Key Lesson: Immediate notification of affected users and financial institutions is critical in payment system breaches.

5.1.7. Best Practice in Transparency: MITRE Breach of 2024

MITRE, a leading cybersecurity research organization, experienced a zero-day exploit targeting

internal systems. Unlike other cases, MITRE swiftly disclosed the breach, provided detailed remediation steps, and shared intelligence with the cybersecurity community to prevent further exploitation [46].

- Best Practice: MITRE's transparent approach minimized misinformation and contributed to industry-wide resilience.
- Key Lesson: Proactive disclosure fosters collective defense in the cybersecurity ecosystem.

5.1.8. Prolonged Crisis Due to Vague Communication: Equifax Breach of 2017

One of the largest data breaches in history, the Equifax breach exposed sensitive personal and financial information of 147 million individuals due to unpatched vulnerabilities in web applications. Equifax delayed public disclosure by six weeks. When it finally announced the breach, its communications lacked clarity, and the company struggled to provide an effective response plan for affected users. Confusing messages about credit monitoring options and responsibility further diminished consumer confidence [47].

- Pitfall: Delayed and vague communication prolonged regulatory scrutiny and reputational damage.
- Key Lesson: Breach notification must be clear, timely, and include actionable remediation guidance for affected individuals.

5.2. Comparative Discussion and Lessons Learned

Table 1. Key Insights from Comparative Analysis.

Case analysis	Timeliness	Message Consistency	Stakeholder Engagement	Regulatory Compliance
CrowdStrike - 2024	Immediate	Consistent	High	Fully Compliant
Costa Rica – 2022	Delayed	Fragmented	Low	Non-Compliant
WannaCry – 2017	Delayed	Inconsistent	Limited	Partial Compliance
Sony Pictures – 2014	Inconsistent	Contradictory	Weak	Inadequate
Uber – 2016	Concealed	Obscured	Weak	Non-Compliant
Target – 2013	Delayed	Inconsistent	Weak	Non-Compliant
MITRE – 2024	Immediate	Consistent	High	Fully Compliant
Equifax - 2017	Delayed	Vague	Limited	Non-Compliant

One of the key insights from the comparative analysis is the importance of timeliness in incident disclosure. Organizations that promptly disclosed incidents, such as CrowdStrike and MITRE, experienced less operational disruption and maintained stronger stakeholder trust. In contrast, cases where disclosure was delayed or concealed, such as Equifax, Uber, Target, and Costa Rica, suffered greater reputational damage and faced significant financial penalties. This underscores the critical role of timely and transparent communication in mitigating the negative impacts of cybersecurity incidents.

Another critical insight is the role of message consistency and transparency in maintaining public confidence. Coordinated messaging, as demonstrated by CrowdStrike and MITRE, helped build trust and manage stakeholder expectations effectively. Conversely, conflicting or misleading statements, as seen in the cases of Sony, Costa Rica, Equifax and WannaCry, resulted in public confusion and a loss of credibility. These examples highlight the need for clear, consistent, and transparent communication to avoid exacerbating the crisis.

The analysis also emphasizes the significance of stakeholder engagement in crisis management. Proactive communication strategies, exemplified by CrowdStrike and MITRE, facilitated collaborative resolution efforts and strengthened stakeholder relationships. In contrast, limited or weak engagement, as observed in the cases of Uber, Costa Rica, Equifax, WannaCry, and Sony, led to misinformation, operational inefficiencies, and regulatory backlash. Effective stakeholder engagement is essential for ensuring a coordinated response and minimizing the long-term impacts of a crisis.

This comparative analysis underscores that organizations with pre-established, transparent, and timely crisis communication frameworks experience faster recovery and stronger stakeholder trust, while those that delay, obscure, or fragment their messaging face increased reputational, regulatory, and financial risks. By integrating communication into cybersecurity incident response strategies, organizations can minimize the impact of cyber incidents, maintain regulatory compliance, and protect public trust in increasingly digital-dependent economies.

6. Incident Response and Communication

Addressing cyber incident response comprehensively requires an understanding of the associated costs, response times, and containment methodologies. In 2024, the global average cost of a data breach rose to $4.88 million, reflecting a 10% increase over the previous year, according to IBM's Cost of a Data Breach Report 2024 [48]. This figure represents breaches across 16 countries and regions and 17 industries. However, breach costs vary significantly by location: the United States recorded the highest average cost at $9.36 million, followed by the Middle East at $8.75 million and Benelux at $5.90 million. In contrast, Latin America reported an average breach cost of $4.16 million, and Brazil had the lowest, at $1.36 million [48]. This escalation in costs is largely driven by operational disruption, customer support expenses, and regulatory fines. Additionally, the time required to identify and contain a breach significantly affects these costs: incidents involving compromised credentials take an average of 292 days to resolve, leading to extensive reputational damage and prolonged operational downtime [49].

Certain industries, such as manufacturing and finance, are particularly vulnerable due to their high exposure to malware and ransomware attacks. In 2024, manufacturing accounted for 25.7% of reported incidents, with malware as the primary attack method at 45% and ransomware at 17%. Ransomware is especially costly and difficult to contain [49]. These figures underscore the necessity for rapid, effective responses, as prolonged identification and containment are directly linked to elevated breach costs. Notably, organizations that lack AI and automation in their security processes experience longer response times and up to 45% higher costs compared to those using these technologies for early threat prevention and detection [48,49].

When a cyber incident occurs, a series of essential questions arise: Who needs to be informed? What assessments must be completed? How can communication be effectively coordinated within and outside the organization? High-profile cases, such as those involving Target and Uber, illustrate the severe repercussions when companies fail to communicate effectively during a cyber incident. In Target's 2013 data breach, delays in internal escalation and public notification contributed to severe reputational damage and financial losses, even though advanced security measures were in place. Similarly, in Uber's 2016 breach, ineffective communication and delayed disclosure led to regulatory penalties and significant public distrust. These cases illustrate that beyond technical defenses,

structured and transparent communication channels, both internally and with external stakeholders, are critical to effectively managing the aftermath of cyber incidents. Incident response is not solely about containment and recovery; it is also about ensuring a timely, accurate flow of information to mitigate damage, uphold trust, and fulfill regulatory obligations [50].

6.1. Theoretical Framework on Incident Response

Incident response frameworks vary significantly across standards, such as ISO/IEC 27035, NIST SP 800-61, and the SANS PICERL model, each providing distinct stages and perspectives tailored to specific organizational needs. For instance, ISO/IEC 27035 divides incident management into five phases: Plan and Prepare, Detect and Report, Assess and Decide, Respond, and Learn Lessons, emphasizing the need for continuous communication and coordination throughout [51-54]. NIST's model, rooted in the Cybersecurity Framework (CSF) 2.0 Functions, categorizes incident response into Detect, Respond, and Recover, while integrating additional governance and improvement phases to support broader cybersecurity management [55]. Conversely, the SANS PICERL model follows a linear process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned [56].

6.1.1. Review of Existing Incident Response Models

Established incident response frameworks form a solid foundation for managing cybersecurity threats by providing systematic approaches that guide organizations through the multifaceted stages of incident management. The ISO/IEC 27035 series, for instance, is widely recognized for its comprehensive structure, which is divided into several interrelated parts. In its first part, the standard introduces fundamental principles and processes essential for effective incident management, placing a strong emphasis on thorough planning and preparedness. The second part builds on this foundation by focusing on the development and implementation of incident response plans, the formation of dedicated incident teams, and the establishment of procedures that incorporate communication protocols. The third part addresses the operational aspects specifically related to ICT incidents, offering systematic methods for detecting, reporting, analyzing, containing, eradicating, and recovering from incidents.

The fourth part of ISO/IEC 27035 highlights the critical importance of coordinated response efforts, underlining the need for efficient information exchange between internal and external stakeholders. Complementing this standard, the NIST SP 800-61 guide introduces a lifecycle approach to incident management, dividing the process into phases that include preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. This model is particularly valued for its iterative process of continuous improvement through lessons learned and for its emphasis on escalating incidents based on severity, ensuring that response capabilities evolve over time.

The SANS PICERL model, by contrast, presents a straightforward and linear approach by organizing incident management into six phases: preparation, identification, containment, eradication, recovery, and lessons learned. Despite their utility and robust methodologies, these models not fully integrating structured communication as a central component, resulting in fragmented communication pathways that may hinder operational effectiveness and slow response times during critical incidents.

6.1.2. Proposed Unified Communication Model for Incident Response

In light of the communication gaps identified in established incident response models, the proposed Unified Communication Model presents an integrated approach that treats communication as an equally critical pillar alongside technical and operational responses. This model is designed around six distinct phases that mirror the core processes of traditional frameworks while embedding structured communication protocols into every stage of the incident response lifecycle. It begins with a phase of Detection and Reporting, where the rapid identification of incidents is immediately coupled with internal notification procedures, ensuring that the entire organization is quickly made aware of potential threats.

This is followed by a Notification and Escalation phase, during which pre-established communication channels are activated to ensure that relevant stakeholders are informed promptly, with the level of alert being proportional to the severity of the incident. As the incident progresses to the Triage and Analysis phase, the model emphasizes the necessity for clear and consistent messaging to guarantee that all decision-makers and operational teams have a unified understanding of the incident's scope and potential impact.

During the Response phase, which encompasses containment, eradication, and recovery, continuous and detailed communication is maintained to keep technical, managerial, and operational teams aligned, thereby reducing the risk of miscommunication or operational missteps. An explicit focus on External Communication and Stakeholder Notifications is also integral to the model, ensuring that regulators, partners, and the public receive timely and accurate information that helps manage the organization's public perception and mitigates reputational risks.

Finally, the model culminates in a Post-Incident Analysis and Lessons Learned phase, during which structured communication is employed to capture feedback from all involved parties, facilitate organizational learning, and refine future incident response protocols. By standardizing communication practices across the entire incident lifecycle, the Unified Communication Model not only enhances interdepartmental coordination and accelerates response times but also reinforces regulatory compliance and preserves stakeholder confidence in today's high-risk digital environment.

This research proposes a unified structure focused specifically on enhancing communication at every stage:

1) Detection and Reporting.
2) Notification and Escalation.
3) Triage and Analysis.
4) Response (Containment, Eradication, and Recovery).
5) External Communication and Stakeholder Notifications.
6) Post-Incident Analysis and Lessons Learned.

Structured communication within this model is intended to ensure that incident management is handled in a coordinated, confidential, and efficient manner, ultimately enhancing organizational resilience and reinforcing stakeholder trust. Moreover, by emphasizing communication, this framework aims to address common gaps identified in high-profile incident response cases, where delayed or unclear communication has compounded the impact of breaches on reputation and financial stability.

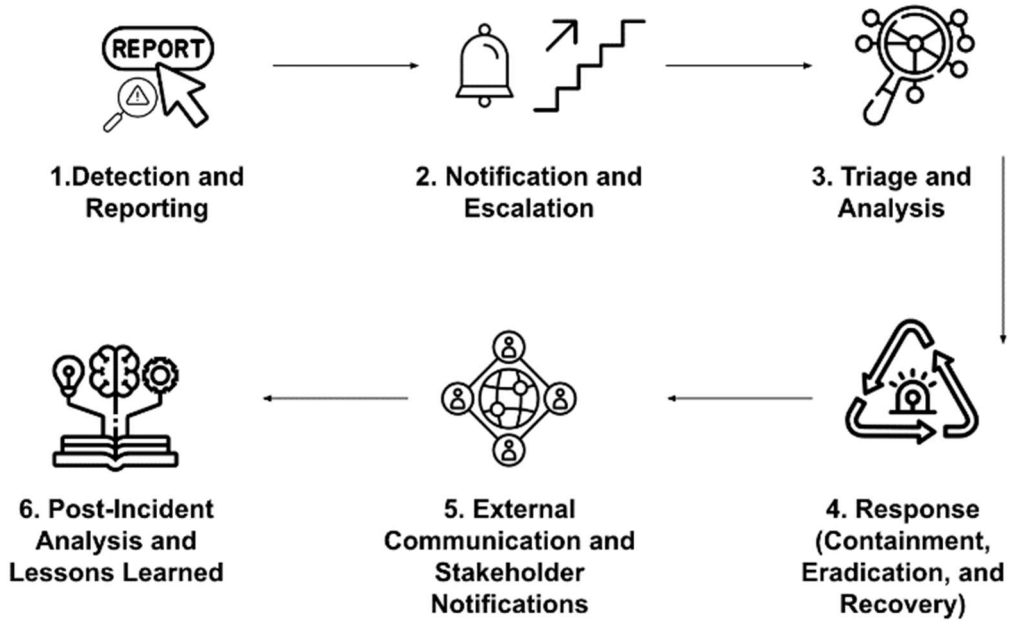

Figure 1. Proposed Unified Incident Response Communication Framework illustrating the following steps: 1. Detection and Reporting; 2. Notification and Escalation; 3. Triage and Analysis; 4. Response (Containment, Eradication, and Recovery); 5. External Communication and Stakeholder Notifications; 6. Post-Incident Analysis and Lessons Learned.

6.1.3. Communication Strategies in Cyber Incident Management

Effective communication is central to cybersecurity incident management, as outlined in ISO/IEC 27035-1:2023. This international standard, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), provides guidelines that are widely adopted by organizations across both the public and private sectors to establish a systematic approach to handling cybersecurity incidents. Clear, coordinated messaging means having a pre-established communication strategy that delivers consistent, accurate, and timely information. For instance, a good practice is to use standardized templates and defined protocols for both internal alerts and external press releases during an incident, ensuring that all team members and stakeholders receive the same verified information at the right time. In contrast, a bad practice would involve disseminating uncoordinated or conflicting messages, which can lead to confusion, misinformation, and a loss of trust.

In particular, the “no-fault” approach to incident reporting encourages staff to report security events without fear of retribution, thereby fostering a culture of openness and continuous improvement [51]. Furthermore, the incident communication process involves not only prompt internal notifications but also controlled external messaging by designated personnel. This coordinated strategy helps maintain transparency while protecting sensitive information, ultimately mitigating potential damage and enhancing long-term resilience.

Continuing from the foundational role of effective communication in incident management, as highlighted in ISO/IEC 27035-1, the planning and preparation phase outlined in ISO/IEC 27035-2:2023 reinforces this focus by advocating for a comprehensive incident management policy. This policy not only defines the organization's objectives and responsibilities but also clarifies the communication channels necessary for efficient incident response [53]. Establishing well-defined protocols and roles

in incident management ensures that all stakeholders, both internal and external, are informed and prepared to respond to cybersecurity threats promptly.

A key aspect of this policy is the integration of communication standards that facilitate information sharing while safeguarding sensitive data. The organization must ensure that all personnel involved in incident management understand how and when to communicate critical information across departments and with external entities, including legal, public relations, and technical teams. By fostering a collaborative environment and providing clear, accessible guidelines, organizations can coordinate their response efforts and mitigate potential damages effectively. Furthermore, having predefined escalation paths ensures that incidents are handled at the appropriate level, allowing for prompt decision-making and resource allocation.

Another critical component of the communication strategy is the emphasis on confidentiality, especially when interacting with external stakeholders such as law enforcement, CERTs, and regulatory bodies. ISO/IEC 27035-2 stipulates the need for controlled communication protocols to ensure that only authorized personnel engage with these parties, maintaining the organization's credibility and protecting its data integrity. In cases of severe incidents, the policy advises using the Traffic Light Protocol (TLP) to label information and clarify sharing permissions, which helps prevent unauthorized disclosure and reduces legal risks [53].

According to ISO/IEC 27035-3:2020, incident notification operations involve structured steps, from the initial detection of a security event to its notification within the organization, and, if necessary, external reporting. This process includes internal reporting to designated Points of Contact (PoC) and potential external notifications, such as to regulatory authorities or affected stakeholders, based on incident severity. By organizing communication through standardized forms and channels, such as CSIRT email addresses or hotlines, organizations can streamline the reporting and handling of incidents, ensuring that critical details are gathered efficiently [51].

Complementing these practices, ISO/IEC FDIS 27035-4:2024 emphasizes a Common Understanding Principle, which advocates for the use of shared terminology and data classification standards across organizations. This common language supports mutual understanding and consistency in communication, crucial when multiple entities are coordinating responses [54].

6.1.4. Practical Communication Steps in Cyber Incident Management.

In this section, we outline general steps for responding to a cyber incident, emphasizing the role of effective communication at each stage of the process. Clear and structured communication is crucial to managing incidents efficiently, ensuring that relevant stakeholders are informed and coordinated throughout the response. Following these foundational steps, a concrete case analysis will be presented to illustrate how these communication-focused strategies can be applied in a real-world scenario, demonstrating their impact on incident resolution and containment. General Steps:

1) Initial Detection and Reporting: Once a potential incident is detected, internal detection mechanisms (like Security Information and Event Management systems) alert the Incident Response Team (IRT) and designated Points of Contact (PoCs). This detection is documented using standardized incident reporting forms, including details about the nature of the alert, system affected, and initial observations. Per ISO/IEC 27035-1, clear documentation helps establish a foundation for managing communication.

2) Notification and Escalation: The designated PoC assesses the incident's severity. If it meets the threshold for escalation, the IRT is formally activated. Here, internal departments, IT, legal, and public relations, are notified according to the ISO/IEC 27035-2 policy guidelines, which emphasize defined roles for each department. Clear escalation paths ensure that relevant stakeholders, including executive management, are informed promptly, allowing them to allocate resources for the incident response.

3) Triage and Analysis (Internal Coordination and Information Sharing): As per ISO/IEC 27035-3, the IRT holds an initial briefing, coordinated by the incident manager, to review current data and decide on containment measures. Communication here is structured around confidentiality needs: departments share information according to the "need-to-know" principle to avoid unnecessary data exposure. Technical, legal, and managerial teams discuss strategies in real time through secure communication channels, such as encrypted emails or designated incident response platforms.

4) Containment, Eradication, and Recovery Updates: During the containment phase, the IRT coordinates actions to limit the incident's impact. Regular status updates are sent to key internal stakeholders, and a summary report is maintained to log actions taken. ISO/IEC 27035-2 recommends that during this phase, external communication should be minimized to avoid unnecessary information leaks. The organization might use the Traffic Light Protocol (TLP) to classify communication based on sensitivity, ensuring sensitive details are shared only with designated personnel.

5) External Communication and Stakeholder Notifications: If the incident impacts external parties (clients or partners), communication guidelines from ISO/IEC 27035-3 are followed. For example, regulated industries might notify relevant authorities or CERTs if there is a significant breach. External messages are carefully crafted by the PR team and legal advisors to ensure compliance with regulatory requirements while preserving the organization's reputation.

6) Post-Incident Reporting and Lessons Learned: After containment and eradication, a comprehensive incident report is compiled, detailing all stages of the response, including a timeline of communication actions taken. ISO/IEC 27035-1 emphasizes a lessons-learned phase, where feedback is collected from all teams involved. The IRT conducts a debrief with management, analyzing communication strengths and areas for improvement, and updates the incident response plan accordingly.

Before delving into the stages to be addressed, let us consider a concrete case analysis: the Uber Hack of 2016. This incident involved two major breaches, both mishandled due to a lack of transparent and structured communication. In the first breach, Uber's then Chief Security Officer, Joseph Sullivan, authorized a USD 100,000 payment to hackers through the company's bug bounty program, accompanied by non-disclosure agreements (NDAs) to conceal the incident. This decision not only obstructed an ongoing FTC investigation but also led to criminal charges against Sullivan. The second breach exposed the data of 57 million users and drivers, yet Uber again chose to pay the hackers to delete the data rather than notifying regulators or affected parties. The delayed disclosure triggered a coordinated legal response across all 50 U.S. states, resulting in a USD 148 million settlement and mandated cybersecurity improvements [44]. These actions underscore the severe legal, financial, and reputational consequences of inadequate communication during cybersecurity incidents.

The table below contrasts the actions taken during the incident with the communication steps that should have been implemented, based on the Practical Communication Steps in Cyber Incident Management.

Table 2. Uber Hack of 2016: the actions taken during the incident with the communication steps that should have been implemented.

Step	What They Did	What They Should Have Done
1. Initial Detection and Reporting	Suspicious activity was detected; however, the incident was not formally documented nor properly reported to the Incident Response Team (IRT) and designated Points of Contact. Instead, the breach was handled quietly without triggering the standard reporting protocols.	Upon detection, internal mechanisms such as SIEM should have generated an immediate alert. The incident should have been documented using standardized reporting forms, detailing the alert's nature, affected systems, and initial observations, in line with ISO/IEC 27035-1, ensuring that the IRT and PoCs were promptly notified.
2. Notification and Escalation	Rather than formally assessing the severity of the breach and escalating it, the then Chief Security Officer authorized payments through the bug bounty program and used non-disclosure agreements to silence the hackers. This action bypassed the established internal notification channels and proper escalation procedures.	The designated PoC should have evaluated the incident's severity and, if necessary, activated the IRT immediately. Internal departments such as IT, legal, and public relations should have been promptly notified according to ISO/IEC 27035-2, ensuring clear escalation paths and proper allocation of resources for an effective incident response.
3. Triage and Analysis (Internal Coordination and Information Sharing)	There was no structured initial briefing to review the information gathered or share critical information among technical, legal, and managerial teams. The lack of coordinated internal communication hindered a comprehensive analysis of the breach.	The IRT should have convened an immediate briefing, coordinated by the incident manager, to share initial analyses securely and on a need-to-know basis. This structured internal coordination would have enabled a timely assessment of the threat and informed the decision-making process for containment measures, as recommended by ISO/IEC 27035-3.
4. Containment, Eradication, and Recovery Updates	Instead of implementing coordinated technical actions, the response relied on financial settlements to have the hackers delete the compromised data. Regular updates to internal stakeholders were not provided, and detailed documentation of containment actions was lacking.	The IRT should have executed a coordinated response for containment, eradication, and recovery. This would have included regular status updates to key internal stakeholders and the maintenance of a summary report logging all actions taken, ensuring that each step was carefully managed and documented in accordance with ISO/IEC 27035-2.
5. External Communication and Stakeholder Notifications	External parties, including regulators and affected users, were not promptly informed. The deliberate concealment of the breach led to a delayed disclosure that eventually triggered a coordinated legal response from state authorities and resulted in significant reputational damage.	External communication protocols should have been followed immediately. Notifications to regulators, clients, and partners should have been issued with carefully crafted messages by PR and legal teams, ensuring compliance with regulatory requirements and protecting the organization's reputation, as advised by ISO/IEC 27035-3.

6. Post-Incident Reporting and Lessons Learned	The focus on concealing the breach prevented a thorough post-incident analysis. As a result, opportunities for learning and process improvement were missed, ultimately culminating in severe financial penalties and long-lasting reputational harm.	A comprehensive incident report should have been compiled after containment and eradication, detailing all response and communication stages. A debrief with management would have allowed for an analysis of communication strengths and weaknesses, with subsequent updates to the incident response plan—thereby fostering organizational resilience and compliance with ISO/IEC 27035-1.

This comparison highlights that proactive, transparent, and coordinated communication is crucial not only for managing the immediate incidents but also for sustaining long-term stakeholder trust and regulatory compliance.

7. Crisis Management and Communication

In the context of cybersecurity, a crisis is not merely any incident, it is defined as an event where the damages and disruptions surpass an organization's normal response capabilities. A cybersecurity incident becomes a crisis when the standard technical procedures (often managed solely by IT) are insufficient, and the incident escalates in severity [57]. This escalation is characterized by extensive operational interruptions, significant financial losses, reputational damage, and even legal or regulatory repercussions. In such scenarios, the organization must go beyond immediate technical fixes and engage in a strategic, holistic response that integrates both technical containment and robust communication measures.

This approach is increasingly reflected in evolving regulatory frameworks. As similar incidents expose systemic vulnerabilities, regulators are now enforcing resilience standards that mandate integrated crisis management and communication protocols. For instance, the European Union's Digital Operational Resilience Act (DORA) not only requires financial institutions to establish rigorous ICT risk management and crisis communication plans, including designating crisis communication coordinators, but also emphasizes the continuous testing of these protocols [58]. Such measures ensure that organizations are not only capable of rapidly containing technical incidents but also prepared to manage public disclosures, media inquiries, and stakeholder communications in real time.

In line with recent EU initiatives, the Cyber Blueprint proposal emphasizes that cyber crisis management should be approached as a shared responsibility, advocating for a non-binding framework that delineates specific, coordinated actions among both civilian and military stakeholders to ensure robust and secure communication throughout the crisis management lifecycle [59].

In contrast to traditional incident response, which is primarily focused on immediate containment, eradication, and system recovery, crisis management adopts a broader, strategic perspective. This integrated approach ensures that, even as technical teams work to restore normal operations, communication strategies keep all stakeholders informed and engaged, laying the groundwork for future resilience.

By defining a crisis as an event that overwhelms conventional response capacities, organizations can better align their internal plans with both technical and communicative strategies. This dual focus

is essential for mitigating the overall impact of cyber incidents and for meeting the demands of increasingly stringent regulatory environments.

7.1. Theoretical Framework on Crisis Management

Effective crisis management requires a structured and adaptable approach, especially when timely and transparent communication can significantly mitigate potential damage. Three key standards provide comprehensive frameworks for managing organizational crises: ISO 22360:2024, ISO 22361:2022, and NIST's Computer Security Incident Handling Guide (SP 800-61r2). While each standard offers unique perspectives, they all emphasize communication as a core component essential to effective crisis response and resilience.

ISO 22360:2024 conceptualizes crisis as a contextual phenomenon that demands a systems approach, incorporating principles such as crisis identification, assessment, and targeted communication. This framework promotes a multi-level response to different types of crises, spanning incidents to full-scale disasters. Key stages include Identification and Assessment (recognizing the crisis and engaging relevant stakeholders), Crisis Intervention (taking control through clear roles and rapid information dissemination), Crisis Communication (ensuring consistent messaging internally and externally), Critical Control Points (implementing interventions to contain the crisis), and Recovery and Restoration (updating stakeholders and guiding the organization toward resolution) [54]. Within ISO 22360, communication serves as a keystone, enabling coordinated action, reinforcing stakeholder confidence, and maintaining transparency.

Similarly, ISO 22361:2022 builds on these concepts with a framework that enhances organizational resilience through systematic crisis management. This standard emphasizes preparation, real-time communication, and post-crisis evaluation to foster a cohesive response that prevents misinformation and public confusion. Key stages include Preparation and Anticipation (establishing readiness through training and strategic communication plans), Assessment and Decision-Making (evaluating the crisis and continuously aligning with stakeholders), Response Execution (implementing the crisis response plan with a focus on consistent external messaging), Recovery and Continuity (communicating progress to stakeholders as operations normalize), and Continual Improvement (reviewing crisis communication strategies to strengthen future response capabilities [60]. ISO 22361 further underscores the importance of ethical and transparent communication to sustain public trust, especially through digital channels where information can spread rapidly.

NIST SP 800-61r2, while rooted in technical incident response, aligns with the communication principles outlined in the ISO standards, particularly in its emphasis on documentation and controlled information flow. This guide offers a structured series of steps, essential in managing high-stakes cyber incidents. The NIST process involves Documenting Everything (recording each action and all evidence), Finding Assistance (working in teams to enhance efficiency), Analyzing Evidence (confirming the incident through comprehensive examination), Notifying Key Personnel (alerting necessary stakeholders like the CIO and security managers), Notifying US-CERT or External Agencies (if required), Stopping the Incident (disconnecting affected systems), Preserving Evidence (backing up and securing critical data), Wiping Out Effects (removing unauthorized materials and restoring systems), Identifying Vulnerabilities (addressing weaknesses to prevent recurrence), Restoring Operations (confirming system recovery), and Creating a Final Report (summarizing

actions, outcomes, and lessons learned) [61]. NIST's approach to crisis handling prioritizes precise communication to ensure that only those who need to know to receive incident-related updates, thus safeguarding both operational integrity and sensitive information.

In integrating these frameworks, a unified model emerges where procedural rigor and communication flexibility intersect. ISO 22360 and ISO 22361 emphasize comprehensive readiness and structured communication flows, while NIST SP 800-61r2 contributes a granular, action-oriented perspective for technical crisis incidents. Together, these standards underscore the necessity of communication at every crisis stage, from initial assessment to recovery, enabling organizations to minimize reputational risks, uphold regulatory obligations, and sustain trust with internal and external stakeholders. Implementing this multi-faceted approach can equip organizations with the resilience needed to navigate complex crises with clarity, control, and transparency.

While these frameworks differ in structure, each highlights essential stages that, when combined, form a comprehensive response. This research proposes a unified structure focused specifically on enhancing communication at every stage:

1) Preparation and Communication Planning.
2) Crisis Identification and Assessment.
3) Initial Internal and External Notification.
4) Crisis Communication Strategy Deployment.
5) Crisis Intervention and Containment.
6) Continuous Communication and Message Coordination.
7) Critical Control Points.
8) Recovery and Restoration.
9) Post-Crisis Review and Analysis.
10) Continuous Improvement and Training.

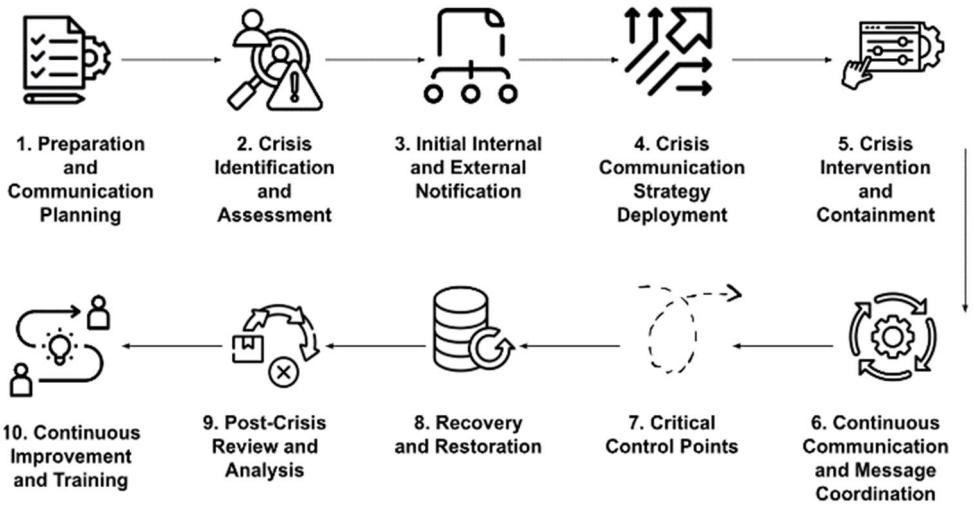

Figure 2. Proposed Unified Crisis Communication Framework, which outlines the following steps: 1. Preparation and Communication Planning; 2. Crisis Identification and Assessment; 3. Initial Internal and External Notification; 4. Crisis Communication Strategy Deployment; 5. Crisis Intervention and Containment; 6. Continuous Communication and Message Coordination; 7. Critical Control Points; 8. Recovery and Restoration; 9. Post-Crisis Review and Analysis; 10. Continuous Improvement and Training.

7.1.1. Effective Communication During a Cybersecurity Crisis

Effective communication is central to crisis management in cybersecurity, requiring organizations to adopt a robust, systematic approach to ensure resilience, accuracy, and coordinated responses. This approach is underscored by a suite of international standards namely, ISO 22360:2024, ISO 22361:2022, ISO 22316:2017, ISO 22301:2019, ISO 28000:2022, ISO 22330:2018, ISO 22313:2020, ISO 22328-2:2024, ISO 22300:2021, and ISO 22320:2018, which collectively guide organizations in establishing effective communication protocols during cyber crises. These standards emphasize that communication during such incidents goes beyond mere information sharing; it plays a critical role in bolstering organizational resilience, supporting swift decision-making, and sustaining stakeholder trust [60,62,63].

ISO 22316:2017 highlights the importance of a coordinated approach, where resilience principles and communication practices are embedded at every organizational level. By aligning governance structures with communication activities, organizations can ensure consistent messaging and enhance decision-making during crises [62]. This standard recommends implementing resilience attributes, such as adaptability and shared values, to support cohesive responses, which is particularly relevant in the cybersecurity landscape, where disruptions can affect multiple internal and external stakeholders [62].

ISO 22301:2019 further reinforces this perspective by integrating communication into the Business Continuity Management System (BCMS). The standard specifies the need for structured communication protocols that outline what information should be conveyed, to whom, and through which channels, both internally and externally [30]. This structure helps prevent misinformation and fosters unified action by ensuring that stakeholders, employees, customers, and partners, receive timely updates aligned with continuity objectives. Moreover, the BCMS framework in ISO 22301:2019 encourages feedback loops to assess and improve communication strategies dynamically as the crisis evolves [64], making it particularly suited for cybersecurity incidents where conditions may shift rapidly.

Security management is also key in crisis communication, as detailed in ISO 28000:2022. This standard emphasizes that security-related risks should be communicated clearly to ensure that all involved parties understand their roles and responsibilities in mitigating these risks [65]. Predefined security communication protocols allow for quick responses, reducing delays that could exacerbate vulnerabilities in a cyber incident. This clarity and alignment are essential to manage both immediate responses and subsequent recovery actions, particularly in high-stakes situations where cybersecurity disruptions can threaten data integrity and organizational reputation [65].

The human dimension of crisis communication is also central to an effective response, as highlighted in ISO/TS 22330:2018. This standard focuses on managing the psychological and behavioral responses of employees and other stakeholders, urging organizations to communicate openly and empathetically during a crisis to maintain trust and morale [66]. Frequent updates help employees understand the evolving nature of the threat, while clarity about their roles in the crisis response empowers them to act responsibly. The standard recognizes that addressing these human factors enhances resilience and ensures that internal teams remain aligned with the broader crisis strategy [66].

External communication is equally vital and must be consistent, transparent, and sensitive to public perception. ISO 22361:2022 outlines best practices for communicating with external audiences,

such as the public, media, and customers, during a crisis [60]. This standard emphasizes that the organization's reputation depends heavily on how it conveys information externally. A well-defined external communication strategy ensures that accurate information reaches stakeholders, preventing rumors and misinformation from gaining traction. This approach is critical in cybersecurity, where a mismanaged public response can quickly erode trust and damage the organization's credibility [60].

ISO 22320:2018 highlights the need for a resilient communication infrastructure, particularly during high-pressure situations that demand a coordinated incident management approach [67]. In cybersecurity crises, having robust communication systems that function under stress is essential for managing the high volumes of information that arise. These systems help synchronize the response across various teams and departments, reducing operational silos and enhancing overall efficiency in managing the incident [67].

In parallel, ISO 22300:2021 introduces the concept of risk communication, underscoring that it should be an ongoing, iterative process involving stakeholders to ensure transparency and informed decision-making [68]. Risk communication aligns the expectations of stakeholders with organizational goals, reinforcing a culture of openness and cooperation that is particularly beneficial in cybersecurity crises, where stakeholders may be concerned about the integrity of sensitive data or the continuity of services [68].

For organizations with direct community-facing roles, ISO 22328-2:2024 provides guidelines for community-based early warning systems that include clear communication strategies. This standard advocates for straightforward, accessible messaging to ensure that critical information reaches all affected parties effectively [69]. This is highly relevant to cybersecurity crises where breaches or disruptions may affect external users, communities, or customer groups, underscoring the organization's commitment to transparency and public safety [69].

ISO 22313:2020 further emphasizes the role of diverse communication channels, advising organizations to use a multi-channel approach to reach relevant audiences effectively during a crisis [36]. In cybersecurity incidents, where rapid information dissemination is crucial, a multi-channel strategy helps ensure uninterrupted communication and allows the organization to manage different audience needs, from employees and stakeholders to external partners and regulatory bodies [70].

Technology's role in crisis communication is particularly highlighted in ISO/TS 22360:2024, which underscores the need for robust, reliable systems that remain operational even under severe disruption [63]. Cybersecurity incidents can compromise digital communication infrastructures, making alternative methods, such as satellite phones, secure backup systems, and dark-site web pages, essential for maintaining information flow. These alternative channels ensure that essential messages are delivered, supporting continuous communication with stakeholders and enabling an adaptable response to evolving cyber threats [63].

In conclusion, effective communication during a cybersecurity crisis is a complex and multi-dimensional process that involves rigorous planning, execution, and continuous improvement. The standards outlined ISO 22316, ISO 22301, ISO 28000, ISO 22330, ISO 22313, ISO 22300, ISO 22320, and others, offer a comprehensive framework that reinforces communication as an integral part of crisis management. By following these guidelines, organizations can establish robust communication protocols that ensure clarity, consistency, and alignment across all levels of response. This structured approach not only enhances operational resilience but also preserves organizational reputation and

stakeholder trust, contributing to a transparent and effective cybersecurity crisis management strategy.

7.1.2. Practical Communication Steps During a Cybersecurity Crisis

In this section, focused on communication in cybersecurity crisis management, we present essential steps to guide effective communication throughout a crisis, ensuring clarity, transparency, and alignment across teams and stakeholders. These steps are designed to establish a structured approach that minimizes impact and maintains trust during incidents. Additionally, a practical case analysis will showcase the application of these communication strategies, providing a real-world perspective on managing a cybersecurity crisis with precision and unified effort. The general steps to address the scenario effectively are listed below.

Table 3. Effective communication steps during a cybersecurity crisis.

Step	Objective	Actions	Outcome
1. Preparation and Communication Planning	Develop a crisis communication plan that establishes roles, procedures, and communication channels	Conduct drills, train staff, and define a media response plan, including spokesperson assignments.	The organization is prepared to respond with clear, consistent messages.
2. Crisis Identification and Assessment	Quickly identify the crisis and assess its potential impact.	Activate a crisis command center, conduct a preliminary assessment to determine severity, and inform key internal stakeholders for early situational awareness.	Initial notifications alert relevant parties, establishing early control.
3. Initial Internal and External Notification	Inform essential personnel and, if necessary, relevant external agencies.	Notify the crisis team, senior management, and, if applicable, external security agencies such as CERT.	Key personnel are alerted, and the situation is under initial control.
4. Crisis Communication Strategy Deployment	Maintain transparency and consistency in communication with stakeholders.	Activate the crisis communication plan, manage public relations, and issue updates to employees, customers, media, and regulators as needed.	Timely, accurate information reaches relevant audiences.
5. Crisis Intervention and Containment	Implement immediate actions to control the situation.	Execute containment measures, while clearly communicating priorities and specific instructions to operational and technical teams.	The crisis is contained, and internal teams understand their roles.
6. Continuous Communication and Message Coordination	Ensure consistent information flow and coordination across all messaging.	Provide regular internal and external updates as needed, maintaining a coherent central message tailored to different audiences.	Aligned, consistent messaging across all channels and stakeholders.
7. Critical Control Points	Implement interventions at decisive points to prevent escalation.	Review messages and adjust them as the crisis evolves, ensuring alignment with key messages.	Narrative control and preventive actions help contain the crisis.
8. Recovery and Restoration	Transition from containment to recovery, keeping stakeholders informed about mitigation and restoration efforts.	Communicate progress updates to stakeholders, and ensure that critical systems return to normal operations.	Normal operations are restored with transparency in the recovery process.

9. Post-Crisis Review and Analysis	Evaluate the crisis response to identify areas for improvement.	Assess the effectiveness of the communication strategy, review areas for improvement, and make adjustments to the crisis plan for enhanced resilience.	A final crisis report outlines lessons learned and recommendations for future responses.
10. Continuous Improvement and Training	Ensure the organization is prepared for future incidents through continuous improvement.	Update the crisis plan, conduct regular drills, and refine communication strategies.	The organization is better equipped for future crises, with strengthened communication strategies.

Let us consider a concrete case analysis: the Target Hack of 2013. This incident, one of the most notorious data breaches in history, compromised the personal data of over 70 million customers and the credit card records of 40 million individuals. Attackers exploited weak network segmentation and a vulnerable vendor system, using phishing and malware to infiltrate Target's critical systems. While the company acted swiftly to secure its environment after detecting the breach, its crisis communication response was severely flawed. Target delayed public disclosure for four days, allowing news of the breach to leak externally before an official statement was issued. This delay, internally justified as necessary for system stabilization, eroded stakeholder trust, amplified reputational damage, and led to high-profile executive resignations and extensive legal repercussions [45]. The Target case underscores that even robust technical defenses can be undermined by ineffective crisis communication strategies, highlighting the critical need for timely, transparent, and coordinated communication in cybersecurity incident management.

Below is a table comparing Target's approach during the 2013 breach with the ideal crisis communication steps based on the Practical Communication Steps During a Cybersecurity Crisis framework:

Table 4. Target's approach during the 2013 breach with the ideal crisis communication steps.

Step	What They Did	What They Should Have Done
1. Preparation and Communication Planning	Target's crisis communication planning was inadequate. While technical response measures were in place, there was no robust, pre-established plan outlining roles, procedures, or media engagement protocols, which left the organization unprepared for timely disclosure.	They should have developed a comprehensive crisis communication plan that clearly defined roles, communication channels, and response procedures, including regular training and simulations, to ensure swift and consistent messaging during an incident.
2. Crisis Identification and Assessment	The breach was detected internally and the focus quickly shifted to technical containment. However, the assessment prioritized system stabilization over evaluating the full impact of the incident on stakeholders and the communication risks involved.	They should have promptly conducted a comprehensive assessment that balanced both technical and communication dimensions, enabling rapid identification of the incident's full scope and the immediate activation of appropriate notification protocols.
3. Initial Internal and External Notification	Although Target secured its environment immediately after detecting the breach, public disclosure was delayed by four days. This delay allowed news to leak externally before an official statement could be issued, undermining stakeholder confidence.	They should have issued immediate notifications to both internal teams and external stakeholders, including regulators, customers, and partners, to control the narrative and maintain trust

		by demonstrating transparency from the outset.
4. Crisis Communication Strategy Deployment	When the breach was eventually announced, the public statement came too late. The belated and inconsistent messaging failed to preempt rumors, allowing speculation to escalate and reputational damage to worsen.	They should have deployed a pre-planned, layered communication strategy immediately upon identifying the breach, ensuring that consistent, transparent, and coordinated messages were disseminated across all channels to manage public sentiment effectively.
5. Crisis Intervention and Containment	Target focused on technical containment by securing its environment but did not adequately communicate these actions. Stakeholders were left uninformed about the measures taken to mitigate the breach, which increased uncertainty.	They should have integrated clear and timely communication of technical interventions with their containment efforts, providing real-time updates that explained the actions being taken to mitigate the breach and reassure all stakeholders.
6. Continuous Communication and Message Coordination	After the delayed disclosure, communication was reactive and sporadic. Inconsistent updates and a lack of coordinated messaging led to confusion and allowed external speculation to flourish.	They should have maintained continuous, coordinated updates with a unified central message tailored to different audiences, ensuring that all stakeholders received regular, accurate, and aligned information throughout the crisis.
7. Critical Control Points	There were no timely interventions at key decision points. The internal justification for delaying disclosure was not matched by any proactive measures to steer the crisis narrative, resulting in significant negative publicity.	They should have leveraged critical control points, such as immediate press briefings or rapid updates during key milestones, to adjust messaging in real time, thereby maintaining narrative control and reassuring stakeholders during decisive moments.
8. Recovery and Restoration	The communication delay compounded the challenges during recovery. Stakeholders remained uncertain about the situation, and the process of restoring trust was hampered by the initial lack of transparency.	They should have initiated recovery communications concurrently with technical restoration, offering clear updates on system improvements and outlining steps taken to prevent future incidents, which would have helped rebuild stakeholder confidence more smoothly.
9. Post-Crisis Review and Analysis	In the aftermath, the delayed and inconsistent communication contributed to significant reputational damage, executive resignations, and extensive legal repercussions, indicating that a thorough review of the communication failures was lacking.	They should have conducted a comprehensive post-crisis review focusing on the effectiveness of the communication strategy, identified lessons learned, and updated their crisis management protocols to prevent similar failures in the future.
10. Continuous Improvement and Training	The incident exposed gaps in crisis communication preparedness. While some improvements may have been made after the breach, the reactive nature of these changes highlighted a failure to prioritize ongoing training and protocol updates before the incident.	They should have embraced a culture of continuous improvement by regularly updating the crisis communication plan, conducting frequent drills and training sessions, and refining strategies to ensure that all personnel are well-prepared to respond effectively to future incidents.

This comparison underscores the critical importance of timely, transparent, and coordinated communication throughout every stage of a cybersecurity crisis to maintain stakeholder trust and effectively manage the incident.

8. Discussion

This research highlights that structured, transparent, and adaptive communication plays a critical role in mitigating the impact of cybersecurity incidents and crises. Organizations that integrate predefined communication protocols within their incident response frameworks, ensuring clarity, timeliness, and stakeholder engagement, demonstrate stronger resilience in managing reputational, operational, and regulatory risks. The comparative analysis of high-profile cybersecurity incidents highlights the profound influence that communication strategies exert on crisis outcomes, revealing that proactive disclosure, message consistency, and strategic external engagement are key determinants in fostering trust and operational continuity.

8.1. Key Contributions and Insights

This research contributes to the growing body of literature on cybersecurity incident management by emphasizing the role of communication as a fundamental pillar rather than a peripheral component. Our analysis reveals several key insights:

1) Timeliness of Disclosure: Incidents where organizations communicated early and clearly (e.g., CrowdStrike Outage, MITRE Breach) experienced less reputational and regulatory fallout compared to cases where delays or concealment exacerbated stakeholder distrust (e.g., Uber Hack, Equifax Breach).

2) Message Consistency and Transparency: Unified, well-coordinated messaging across internal and external stakeholders proved essential in controlling the crisis narrative, whereas fragmented or contradictory statements (e.g., Costa Rica Ransomware Attack, WannaCry) led to uncertainty and misinformation.

3) Stakeholder Engagement and Regulatory Compliance: Entities that actively engaged regulators, customers, and the public in a structured and transparent manner minimized long-term reputational and financial damages. The alignment of communication strategies with regulatory mandates (e.g., GDPR, DORA, CIRCIA) was particularly beneficial in ensuring compliance and mitigating legal risks.

The research underscores that cybersecurity communication should not be reactive or improvised but embedded within an organization's incident response planning. Predefined protocols, secure escalation channels, and stakeholder mapping enhance an entity's ability to respond effectively to crises, protecting both operational integrity and public confidence.

8.2. Limitations of the Research

While this research offers valuable insights into cybersecurity communication strategies, several limitations should be acknowledged:

- Selection Bias in Case Analysis: The research primarily examined well-documented cybersecurity incidents with publicly available information. This focus may introduce selection bias, as organizations that effectively manage communications may be overrepresented, while cases of poor communication without media exposure remain underreported.
- Generalizability Constraints: The evidence is drawn from a mix of corporate, governmental, and critical infrastructure incidents, each subject to distinct legal, operational, and organizational constraints. Therefore, the applicability of the identified best practices may vary across different

industries and regulatory environments.

- Limited Empirical Validation: Although qualitative thematic analysis provided structured insights, the research does not incorporate quantitative assessments to measure the direct impact of communication strategies on reputational recovery or financial losses.
- Regulatory Variability: While this research considers regulatory frameworks such as GDPR, DORA, and CIRCIA, the evolving nature of cybersecurity disclosure requirements presents challenges in formulating universally applicable recommendations. Future research should explore cross-jurisdictional variations and their implications for cybersecurity communication policies.

8.3. Policy and Practical Implications

The insights of this research have significant implications for both regulatory bodies and organizational cybersecurity practices.

- For Organizations:
  - Institutionalizing structured communication frameworks within cybersecurity incident response plans is imperative. Organizations should establish predefined escalation pathways, message templates, and spokesperson roles to ensure coherent, legally compliant, and effective communication during crises.
  - Regular simulation exercises incorporating cross-functional teams (legal, IT, PR, and executive leadership) can enhance preparedness for real-world cyber incidents.
  - Transparent, proactive disclosure strategies, aligned with regulatory mandates, should be prioritized to maintain stakeholder trust and mitigate reputational risks.
- For Policymakers and Regulators:
  - The alignment of incident disclosure regulations across jurisdictions would reduce compliance complexity for multinational organizations. Regulatory bodies should seek harmonization in defining reportable incidents, notification timelines, and disclosure formats.
  - Governments and regulatory agencies (e.g., CISA under CIRCIA, European Authorities under GDPR and DORA) should explore mechanisms that incentivize early incident reporting, such as safe harbor provisions or coordinated response support.
  - Clearer guidelines on public communication expectations during cyber incidents, detailing thresholds for disclosure and best practices for messaging, would benefit both organizations and regulators in crisis response coordination.

This research reinforces that communication is not ancillary but central to cybersecurity incident response and crisis management. Through the integration of structured communication protocols, organizations can navigate complex cyber threats more effectively, ensuring regulatory compliance while preserving stakeholder trust. Future research should further explore empirical methodologies to quantify the impact of strategic communication in cybersecurity crises, as well as the role of emerging technologies, such as AI-driven crisis response tools, in enhancing organizational resilience. By embedding communication as a core element of cybersecurity frameworks, organizations can better prepare for, respond to, and recover from the inevitable cyber challenges of the digital era.

9. Conclusions

This research underscores the critical role of structured communication in cybersecurity incident response and crisis management. Through an in-depth analysis of case studies, regulatory

frameworks, and industry standards, it demonstrates that integrating predefined communication protocols enhances resilience, mitigates reputational and financial risks, and strengthens stakeholder trust. The research highlights that timely disclosure, message consistency, and proactive stakeholder engagement are essential in controlling crisis narratives and ensuring regulatory compliance. While existing incident response frameworks provide robust technical guidance, they often lack explicit communication strategies, a gap addressed by this research's proposed unified communication model.

By embedding structured communication within cybersecurity frameworks, organizations can navigate cyber crises more effectively, preserve operational continuity, and maintain public confidence. Future research should explore empirical validation of these strategies, cross-industry comparative analyses, and the potential role of AI-driven communication tools in automating crisis messaging. As cyber threats continue to evolve, integrating adaptive and transparent communication practices will remain fundamental to strengthening organizational resilience and regulatory alignment.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

[1] Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, 99, 102036. https://doi.org/10.1016/j.cose.2020.102036

[2] Manley, B., & McIntire, D. (2020). A guide to effective incident management communications. CERT Division, Carnegie Mellon University. Available online: https://apps.dtic.mil/sti/trecms/pdf/AD1117526.pdf

[3] Østby, G., & Katt, B. (2020). Cyber crisis management roles – A municipality responsibility case study. In Y. Murayama, D. Velev, & P. Zlateva (Eds.), Information technology in disaster risk reduction: ITDRR 2019 (IFIP Advances in Information and Communication Technology, Vol. 575, pp. 168–181). Springer, Cham. https://doi.org/10.1007/978-3-030-48939-7_15

[4] Reinhold, A. M., Gore, R. J., Ezell, B., Izurieta, C. I., & Shanahan, E. A. (2025). From cyclones to cybersecurity: A call for convergence in risk and crisis communications research. Journal of Homeland Security and Emergency Management, 12(3), 1–20. https://doi.org/10.1515/jhsem-2023-0067

[5] Citrawijaya, O. R., Susanto, B. K., & Amalia, D. A. (2024). The role of communication strategies in crisis management: A comparative analysis across industries. The Journal of Academic Science, 1(6), 748–761. https://doi.org/10.59613/cej49p88

[6] Ruohonen, J., Hjerppe, K., & Kortesuo, K. (2024). Crisis communication in the face of data breaches [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2406.01744

[7] Backman, S. (2021). Conceptualizing cyber crises. Journal of Contingencies and Crisis Management, 29(4), 429–438. https://doi.org/10.1111/1468-5973.12347

[8] Bolton, F. (2013). Cybersecurity and emergency management: Encryption and the inability to communicate. Journal of Homeland Security and Emergency Management, 10(1), 379–385. https://doi.org/10.1515/jhsem-2012-0038

[9] Mott, G., Nurse, J. R. C., & Baker-Beall, C. (2023). Preparing for future cyber crises: Lessons from governance of the coronavirus pandemic. Policy Design and Practice, 6(2), 160–181. https://doi.org/10.1080/25741292.2023.2205764+

[10] Ramadhianto, R., Toruan, T. S. L., Kertopati, S. N. H., & Almubaroq, H. Z. (2023). Analysis of presidential regulations concerning cyber security to bolster defense policy management. Defense and Security Studies, 4, 84–93. https://doi.org/10.37868/dss.v4.id244

[11] Grosu, I. -P., Dinicu, A. -E., Lupédia, G. D. C., & State, C. (2023). Managing crisis situations for performance enhancement: A scientific inquiry. In Proceedings of the 17th International Management Conference

"Management beyond Crisis: Rethinking Business Performance" (Vol. 17, No. 1, pp. 49–60). Faculty of Management, Academy of Economic Studies, Bucharest, Romania. https://doi.org/10.24818/IMC/2023/01.05

[12] Sikder, A. S., & Harvey, K. (2023). Techno-resilience: Unraveling the impact of cutting-edge information technology in crisis management and emergency response for enhanced disaster preparedness and response efficiency. International Journal of Information Science and Technology, 1(1), 138–169. https://doi.org/10.70774/ijist.v1i1.17

[13] Mahmood, S., Chadhar, M., & Firmin, S. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. Journal of Contingencies and Crisis Management, 32(1), e12549. https://doi.org/10.1111/1468-5973.12549

[14] Moerschell, L., & Novak, S. S. (2020). Managing crisis in a university setting: The challenge of alignment. Journal of Contingencies and Crisis Management, 28(1), 30–40. https://doi.org/10.1111/1468-5973.12266

[15] Steen, R., Haug, O. J., & Patriarca, R. (2024). Business continuity and resilience management: A conceptual framework. Journal of Contingencies and Crisis Management, 32(1), e12501. https://doi.org/10.1111/1468-5973.12501

[16] Kiiveri, K., Naumanen, P., Liesivuori, J., Virtanen, S., & Isoaho, J. (2024). A four-phase model and a mobile app for crisis preparedness and management in small and medium-sized enterprises. Journal of Contingencies and Crisis Management, 32(3), e12618. https://doi.org/10.1111/1468-5973.12618

[17] Liu, T., Zhang, H., Li, X., & Li, H. (2016). The effects of the social context on pre-decisional processes of protective action in Beijing communities. Journal of Risk Analysis and Crisis Response, 6(1), 21-30. https://doi.org/10.2991/jrarc.2016.6.1.4

[18] Yang, Y., Jin, L., Li, J., & Fang, C. (2015). Crisis communication about nuclear accidents with psychological approaches. Journal of Risk Analysis and Crisis Response, 5(3), 169-177. https://doi.org/10.2991/jrarc.2015.5.3.4

[19] Sparf, J., & Öhman, S. (2014). On risk and disability – Investigating the influence of disability and social capital on the perception and digital communication of risk. Journal of Risk Analysis and Crisis Response, 4(1), 20-33. https://doi.org/10.2991/jrarc.2014.4.1.3

[20] Nussipova, A., Khussainova, G., Kabilova, R., Aliyarov, E., & Nuralina, B. (2024). Information security communications strategy as a prerequisite to counteracting hybrid warfare: World experience. Revista Latina de Comunicación Social, 82, 1–20. https://doi.org/10.4185/rlcs-2024-2134

[21] Tähtinen, L., Toivonen, S., & Rashidfarokhi, A. (2024). Landscape and domains of possible future threats from a societal point of view. Journal of Contingencies and Crisis Management, 32(1), e12529. https://doi.org/10.1111/1468-5973.12529

[22] Borden, J., Zhang, X. A., & Hwang, J. (2020). Improving automated crisis detection via an improved understanding of crisis language: Linguistic categories in social media crises. Journal of Contingencies and Crisis Management, 28(3), 281–290. https://doi.org/10.1111/1468-5973.12308

[23] Zhan, M. M., & Zhao, X. (2021). How stakeholders react to issues with risk implications: Extending a relational perspective of issues management. Journal of Contingencies and Crisis Management, 29(4), 385–398. https://doi.org/10.1111/1468-5973.12359

[24] Moral, P. (2023). Restoring reputation through digital diplomacy: The European Union's strategic narratives on Twitter during the COVID-19 pandemic. Communication & Society, 36(2), 241–269. https://doi.org/10.15581/003.36.2.241-269

[25] Manfredi, J. -L., Amado, A., & Gómez-Iniesta, P. (2022). State disinformation: Emotions at the service of the cause. Communication & Society, 35(2), 205–221. https://doi.org/10.15581/003.35.2.205-221

[26] Department of Homeland Security. (2013). NIPP 2013 Partnering for Critical Infrastructure Security and Resilience. Available: https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

[27] European Parliament and Council. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, 164–198. Available online: http://data.europa.eu/eli/dir/2022/2557/oj

[28] European Parliament and Council. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU)

2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, p. 80. Available online: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

[29] Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503–506. https://doi.org/10.1016/j.procs.2015.04.126

[30] Hooper, V., & McKissack, J. (2016). The emerging role of the CISO. Business Horizons, 59(6), 585–591. https://doi.org/10.1016/j.bushor.2016.07.004

[31] Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. Journal of Cybersecurity, 8(1), tyac006. https://doi.org/10.1093/cybsec/tyac006

[32] Lelewski, R., & Hollenberger, J. (2024). Cybersecurity tabletop exercises: From planning to execution. No Starch Press.

[33] Basheer, R., & Alkhatib, B. (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. Journal of Computer Networks and Communications, 2021, 1302999. https://doi.org/10.1155/2021/1302999

[34] Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

[35] Consolidated Appropriations Act. (2022). H.R. 2471, 117th Cong., Public Law No. 117-103. https://www.congress.gov/bill/117th-congress/house-bill/2471

[36] U.S. Securities and Exchange Commission. (2024). Disclosure of cybersecurity incidents determined to be material and other cybersecurity incidents. Available online: https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024

[37] European Parliament and Council. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union, L 2024/2847, 1–XX. Available online: http://data.europa.eu/eli/reg/2024/2847/oj

[38] Cybersecurity and Infrastructure Security Agency. (2020). Binding operational directive 20-01: Develop and publish a vulnerability disclosure policy. Available online: https://www.cisa.gov/binding-operational-directive-20-01

[39] Nussipova, A., Khussainova, G., Kabilova, R., Aliyarov, E., & Nuralina, B. (2024). Information security communications strategy as a prerequisite to counteracting hybrid warfare: World experience. Revista Latina de Comunicación Social, 82, 1–20. https://doi.org/10.4185/rlcs-2024-2134

[40] Financial Conduct Authority (FCA). (2024, October 31). CrowdStrike outage: Lessons for operational resilience. Financial Conduct Authority. Available online: https://www.fca.org.uk/firms/operational-resilience/crowdstrike-outage-lessons-operational-resilience (accessed on February 24, 2025)

[41] Burgess, M. (2022, June 12). Conti's attack against Costa Rica sparks a new ransomware era. Wired. Available online: https://www.wired.com/story/costa-rica-ransomware-conti/ (accessed on February 25, 2025)

[42] Prevezianou, M. F. (2021). WannaCry as a creeping crisis. In A. Boin, M. Ekengren, & M. Rhinard (Eds.), Understanding the creeping crisis (pp. 37–50). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-70692-0_3

[43] Schmitt, M. (2014, December 17). International law and cyber-attacks: Sony v. North Korea. Just Security. Available online: https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ (accessed on February 25, 2025)

[44] Dempsey, J. X., & Carlin, J. P. (2024). Cybersecurity law fundamentals (2nd ed.). International Association of Privacy Professionals (IAPP).

[45] Steinberg, S., Stepan, A., & Neary, K. (n.d.). Target cyber-attack: A Columbia University case study. Columbia University School of International and Public Affairs (SIPA). Available online: https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf (accessed on February 25, 2025)

[46] Kass, D. H. (2024, May 1). MITRE shares lessons learned from breach. MSSP Alert. Available online: https://www.msspalert.com/news/mitre-cyber-strike-offers-lessons-on-response-remediation (accessed on February 24, 2025)

[47] Kabanov, I., & Madnick, S. (2021). Applying the lessons from the Equifax cybersecurity incident to build a better defense. MIS Quarterly Executive, 20(2), 109–125. https://doi.org/10.17705/2msqe.00044

[48] IBM. (2024). Cost of a Data Breach Report 2024. Available online: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

[49] IBM. (2024). X-Force Threat Intelligence Index 2024. Available online: https://www.ibm.com/downloads/documents/us-en/107a02e952c8fe80

[50] Dempsey, J. X., & Carlin, J. P. (2024). Cybersecurity law fundamentals (2nd ed.). International Association of Privacy Professionals (IAPP).

[51] ISO. (2020). ISO/IEC 27035-3:2020 Information technology — Information security incident management Part 3: Guidelines for ICT incident response operations. Available online: https://www.iso.org/es/contents/data/standard/07/40/74033.html

[52] ISO. (2023). ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process (Edition 2). Available online: https://www.iso.org/standard/78973.html

[53] ISO. (2023). ISO/IEC 27035-2:2023 Information technology — Information security incident management Part 2: Guidelines to plan and prepare for incident response (Edition 2). Available online: https://www.iso.org/standard/78974.html

[54] ISO. (2024). ISO/IEC FDIS 27035-4 Information technology — Information security incident management Part 4: Coordination. Available online: https://www.iso.org/standard/80973.html

[55] National Institute of Standards and Technology. (2024). NIST Special Publication 800-61r3 ipd Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. https://doi.org/10.6028/NIST.SP.800-61r3.ipd

[56] SANS. (2016). SANS 504-B Incident Response Cycle: Cheat-Sheet v1.0. Available online: https://www.sans.org/media/score/504-incident-response-cycle.pdf

[57] INCIBE. (2024, December 17). Guía de gestión de crisis de ciberseguridad en empresas. INCIBE. Available online: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_gestion_de_crisis.pdf (accessed on February 25, 2025)

[58] European Parliament and Council. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Official Journal of the European Union, L 333, 1–79. Available online: http://data.europa.eu/eli/reg/2022/2554/oj

[59] European Commission. (2025, February 24). Cyber Blueprint – Proposal Council Recommendation. European Commission Newsroom. Available online: https://ec.europa.eu/newsroom/dae/redirection/document/113086 (accessed on February 24, 2025)

[60] ISO. (2022). ISO 22361:2022 Security and resilience — Crisis management — Guidelines. Available online: https://www.iso.org/standard/50267.html

[61] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (SP 800-61r2) [Special Publication]. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

[62] ISO. (2017). ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes. Available online: https://www.iso.org/standard/50053.html

[63] ISO. (2024). ISO/TS 22360:2024 Security and resilience — Crisis management — Concepts, principles, and framework. Available online: https://www.iso.org/standard/50266.html

[64] ISO. (2019). ISO/DIS 22301:2019 Security and resilience — Business continuity management systems — Requirements. Available online: https://www.iso.org/standard/75106.html

[65] ISO. (2022). ISO 28000:2022 Security and resilience — Security management systems — Requirements. Available online: https://www.iso.org/standard/88413.html

[66] ISO. (2018). ISO/TS 22330:2018 Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity. Available online: https://www.iso.org/standard/50067.html

[67] ISO. (2018). ISO 22320:2018 Security and resilience — Emergency management — Guidelines for incident management. Available online: https://www.iso.org/standard/67851.html

[68] ISO. (2021). ISO 22300:2021 Security and resilience — Vocabulary. Available online: https://www.iso.org/standard/77008.html

[69] ISO. (2024). ISO 22328-2:2024 Security and resilience — Emergency Management Part 2: Guidelines for the implementation of a community-based early warning system for landslides. Available online: https://www.iso.org/standard/83417.html

[70] ISO. (2020). ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301. Available online: https://www.iso.org/standard/75107.html

(Executive Editor: Yan Li)