Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Cyber Crisis Communication in Humanitarian Organizations: A Comparative Content Analysis of WFP and ICRC Responses to Data Breaches

ibrahim ukka

ibrahim.okh@najah.edu

An-Najah National University

Doha mezyed

An-Najah National University

aya Hawwash

An-Najah National University

Febriansyah Indra

An-Najah National University

Article

Keywords: cyber crisis communication, humanitarian organizations, data breach, Situational Crisis Communication Theory, Image Repair Theory, protection-bounded transparency, comparative content analysis

Posted Date: November 18th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10931702/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Cyber Crisis Communication in Humanitarian Organizations: A Comparative Content Analysis of WFP and ICRC Responses to Data Breaches

Abstract

Humanitarian organizations increasingly depend on digital registration and data-management systems to deliver aid, a dependence accompanied by rising exposure to cyberattacks against conflict-affected and displaced populations. This study undertakes a qualitative comparative content analysis of the crisis communication responses of two major humanitarian actors - the International Committee of the Red Cross (ICRC), following its 2021-2022 data breach affecting more than 515,000 people, and the World Food Programme (WFP), following its 2026 breach of the Self-Registration Application for Palestine affecting approximately 600,000 Gaza households. Initial source verification indicates that both cases are independently documented and sufficiently comparable for a preliminary comparative analysis, while important differences in temporal observability remain: the ICRC corpus spans a documented communication trajectory from January to at least June 2022, while the WFP corpus, as currently assembled, spans four confirmed official communications issued between 31 May and 9 June 2026. Drawing on organizations' official communications, coded inductively across an evidence-linked scheme before engagement with Situational Crisis Communication Theory (SCCT) and Image Repair

Theory (IRT), the analysis identifies a shared underlying sequence - acknowledgement, containment, corrective action, beneficiary guidance, and continuity assurance - alongside a divergence in how each organization treats the limits of its own disclosure. The ICRC corpus documents an accountability- and explanation-centered pattern in which limited disclosure is accompanied by an explicit, organization-stated protective rationale, termed here protection-bounded transparency. The WFP corpus, extended through 29 July 2026, documents comparably limited disclosure - including an internal staff directive to avoid technical explanation of the incident - without an equivalent stated rationale, a pattern termed institutional reticence and explicitly contested as unjustified by external stakeholders. The study proposes a preliminary Humanitarian Cyber Crisis Communication and Protection Framework (HCCCPF), organized around a central Protection Boundary construct requiring organizations to state, not merely enact, the rationale for any limits on disclosure. This framework is offered as an evidence-grounded but provisional contribution, pending closure of the full communication corpus for both cases.

Keywords

cyber crisis communication; humanitarian organizations; data breach; Situational Crisis Communication Theory; Image Repair Theory; protection-bounded transparency; comparative content analysis

1. Introduction

The digitalization of humanitarian assistance has transformed how organizations identify, register, and serve affected populations, but it has simultaneously created new categories of risk. Self-registration platforms, biometric identity systems, and beneficiary databases now hold sensitive information about people often experiencing displacement, conflict, detention, family separation, or other forms of heightened vulnerability. When such systems are breached, the population whose data has been exposed is frequently the same population the organization exists to protect, and the geopolitical context in which the breach occurs can compound the risk to affected individuals.

Two cases illustrate this dynamic with unusual clarity and documentary depth. The ICRC determined on 18 January 2022 that servers holding data belonging to more than 515,000 people - connected to its Restoring Family Links program across more than 60 National Societies - had been compromised; its own subsequent analysis traced the intrusion to 9 November 2021. More than four years later, WFP confirmed that its Self-Registration Application for Palestine had been breached on 14 May 2026, exposing the names, identification numbers, phone numbers, and location data of approximately 600,000 Gaza households, with independent reporting also documenting a whistleblower warning to WFP two days before the attack. Both organizations occupy comparable

positions within the international humanitarian system, and both breaches affected populations already made vulnerable by conflict and displacement.

2. Research Problem

Existing crisis communication theory - most influentially Situational Crisis Communication Theory (SCCT; Coombs, 2007) and Image Repair Theory (IRT; Benoit, 2015) - was developed primarily from, and validated against, corporate and political crises in which the organization's central communicative obligation is to its own reputation. Humanitarian organizations operate under a different mandate: their communicative obligation runs first to affected populations who may have limited alternative access to essential assistance, and whose vulnerability is precisely what a data breach threatens to compound. Whether existing frameworks adequately account for this ethical asymmetry between a humanitarian organization and the people it serves remains insufficiently examined empirically.

3. Research Gap

A recent PRISMA-ScR scoping review of cybersecurity in humanitarian operations found that, while cyber threats and preparedness gaps in the sector are increasingly documented, the literature remains limited on crisis communication strategies specifically following cyber incidents in humanitarian settings (Anfuso et al., 2026). Parallel literature on

corporate data-breach crisis communication - including SCCT-based comparative and computational studies (Kuipers & Schonheit, 2022; Jechle et al., 2025) - offers a developed but sector-specific body of findings that has not yet been systematically tested against humanitarian cases. This study addresses four interlocking gaps: a theoretical gap (limited testing of SCCT/IRT outside commercial contexts), a contextual gap (the identified scarcity of humanitarian-sector cyber crisis communication research), an empirical gap (few studies grounded in actual organizational communication corpora rather than survey or experimental data), and a methodological gap (limited comparative document-based analysis across humanitarian organizations).

4. Research Questions

Main Research Question: How do humanitarian organizations communicate with affected populations and stakeholders following a cyberattack that compromises beneficiary data, and how do these strategies compare across organizations and contexts?

RQ1: How do the ICRC and WFP acknowledge and disclose the occurrence, scope, and nature of their respective data breaches?

RQ2: Where reliable timestamps are available, how do the two organizations differ in the timing, channel selection, and consistency of breach-related communication?

RQ3: How do the two organizations frame responsibility, and what corrective and protective measures do they communicate to affected populations?

RQ4: To what extent do the identified communication patterns align with, extend, or challenge SCCT and Image Repair Theory when applied to a humanitarian, rather than corporate, context?

Table 1 (RQ Alignment Audit) traces each research question to the specific codes, data sources, and manuscript sections that answer it, so that the correspondence between questions asked and evidence delivered is auditable rather than asserted.

Table 1. Research Question Alignment Audit

RQ	Variables/codes	Data source	Results section	Discussion section	Framework component
RQ1 - acknowledgement & disclosure	CA, ISD, TE	Master Coding Matrix (Section 12.7); Evidence Corpus (Section 12.2-12.3)	13.1, 13.2	14 (first two paragraphs)	Phase 2 (Initial Communication)
RQ2 - timing, channel, consistency	Documented response interval; Communication channels; timeline dates	Verified Comparative Timeline (Section 11); Master Corpus Table	13.1-13.3; Figure 2	14 (institutional reticence discussion)	Phase 1 (Detection & Verification)
RQ3 - responsibility framing, corrective/protective measures	RAF, CoA, BPG, PBR	Master Coding Matrix; ICRC/WFP	13.1-13.3; Figure 1	14 (protection-bounded transparency	Phase 3 (Accountability & Protection Boundary)

		Evidence Tables		vs. institutional reticence)	
RQ4 - alignment/extension/challenge to SCCT and IRT	All codes, interpreted theoretically	Section 8 (Theoretical Framework); Section 7.1 synthesis; Theoretical Construct Synthesis Table 3 (this section)	N/A - RQ4 is answered in Discussion, not Results, consistent with the qualitative design's separation of description from interpretation	14 (entire section)	Phases 3-4; overall HCCCPF rationale (Section 15)

Source: Author's own analysis, tracing each research question to its coding categories, data source, and manuscript section (Sections 4, 12-15).

5. Objectives

1. To conduct a systematic, evidence-linked comparative content analysis of the ICRC (2021-2022) and WFP (2026) crisis communications following their respective data breaches.

2. To identify inductively emergent themes in humanitarian cyber crisis communication before evaluating them against SCCT and IRT.

3. To critically assess the explanatory adequacy of SCCT and IRT in a humanitarian, beneficiary-facing context.

4. To develop and theoretically justify a preliminary, evidence-derived Humanitarian Cyber Crisis Communication and Protection Framework (HCCCPF).

5. To generate practical, finding-linked recommendations for humanitarian organizations managing cyber crisis communication under conditions of population vulnerability.

6. Significance of the Study

Theoretically, the study contributes an empirically grounded test of two dominant crisis communication frameworks in an under-researched organizational context, addressing a gap identified in recent humanitarian cybersecurity literature (Anfuso et al., 2026). Practically, the findings are intended to be usable by humanitarian communication and data-protection officers designing breach-response protocols. The study's humanitarian significance lies in foregrounding a population - conflict-displaced, aid-dependent individuals - whose data-protection needs are rarely centered in crisis communication scholarship, which has predominantly examined corporate and reputational outcomes.

7. Literature Review

7.1 Narrative Synthesis

Crisis communication scholarship examines how organizations manage reputational and operational threat under uncertainty. Coombs (2007) frames crisis response as centrally about managing attributions of responsibility. Corporate data-breach research applying SCCT finds that organizations relying on a single, consistent strategy outperform those blending inconsistent strategies, with denial consistently the most

damaging approach (Kuipers & Schonheit, 2022); computational extensions of SCCT to large breach-disclosure corpora find that firms frequently combine compensation and victimage framing with apology and justification (Jechle et al., 2025). A qualitative study of Finnish data-breach cases similarly finds that early communication, responsibility acceptance, apology, and authority notification distinguish successful from unsuccessful responses (Ruohonen et al., 2024), while sector-specific work on health-service providers documents apology and compensation as recurring post-breach strategies (Masuch et al., 2021). A recent systematic review synthesizes antecedents and consequences of data breaches across the information-systems literature more broadly (Schlackl et al., 2022). Meta-analytic work confirms that attributed responsibility significantly shapes reputational outcomes across SCCT studies (Avery & Park, 2016).

Directly relevant to this study, Choi, Robinson, Ruddle and Fister (2025) explicitly analyze the 2022 ICRC data breach as an illustrative case within a comparative government/nonprofit/for-profit framework, finding that 'rebuild' strategies - responsibility acceptance, apology, and corrective action - are associated with stronger trust restoration across sectors, including humanitarian organizations; this is the closest peer-reviewed treatment of the ICRC case identified, though it does not conduct document-level comparative analysis or examine WFP. Systematic-review work on trust repair in health crises identifies

recurring public-trust-repair mechanisms that parallel several categories in this study's codebook (Liu & Duarte, 2023).

Benoit's (2015) Image Repair Theory offers a complementary typology of denial, evasion, reducing offensiveness, corrective action, and mortification, oriented toward image protection rather than beneficiary welfare - a limitation salient when the harmed party is aid-dependent rather than a paying customer. Stakeholder-oriented crisis communication scholarship argues that mission-driven organizations must address a broader and more differentiated stakeholder set than corporate models assume (Ndlela, 2019), a claim illustrated empirically in stakeholder-differentiated crisis response during the Brussels terror attacks (Marynissen & Lauder, 2020) and conceptually in portfolio-based treatments of crisis strategy selection (Nöhammer et al., 2023). Nonprofit-sector crisis communication research specific to the COVID-19 pandemic similarly suggests corporate-derived frameworks apply only partially to mission-driven organizations (Fuller et al., 2022).

The humanitarian-specific literature on crisis communication remains thin, though adjacent literatures are more developed. The recent scoping review by Anfuso et al. (2026) explicitly identifies crisis communication as an underexamined dimension of humanitarian cybersecurity. A growing critical digital-humanitarianism literature frames data collection as now central, rather than incidental, to humanitarian action (Aradau, 2023), documents surveillance risks associated with digitized

beneficiary systems (Masiero, 2023), and reviews innovation trends including data-driven tools across the sector (Bruder & Baar, 2024). Work on humanitarian data governance frames it as fundamentally a matter of relationships, trust, and ethics rather than compliance alone (Fast, 2023), while more recent governance scholarship debates whether ethical self-regulation is sufficient or whether stronger legal and political control of humanitarian data is required (Lidén, 2026) - a debate with direct bearing on how this study's protection-bounded transparency and institutional reticence constructs might generalize. Humanitarian information-sharing research identifies structural barriers and opportunities distinct from corporate information environments (Nair et al., 2022).

Finally, general crisis-communication scholarship has only recently begun to treat privacy as a first-order concern rather than an afterthought (Watson & Rodrigues, 2017), while legal scholarship on data breaches frames them as a distinct mass-intrusion harm not fully captured by traditional privacy-tort conceptions (Mills, 2017) - a framing consistent with this study's treatment of disclosure limits as potentially protective rather than merely evasive. Table 2 (Literature Matrix) summarizes the studies most directly informing this review; the reference list contains the full set of sources consulted.

7.2 Literature Matrix

Table 2. Literature Matrix

Theme	Study	Context/Method	Key finding relevant to this study
SCCT foundations	Coombs (2007)	Theoretical	Response strategy should be calibrated to crisis type and attributed responsibility
SCCT + data breach	Kuipers & Schonheit (2022)	Comparative corporate case analysis	A single consistent strategy outperforms mixed strategies; denial is consistently most damaging
SCCT + data breach	Choi, Robinson, Ruddle & Fister (2025)	Comparative government/nonprofit/for-profit analysis; explicitly discusses the 2022 ICRC breach as an illustrative case	'Rebuild' strategies (responsibility acceptance, apology, corrective action) are associated with stronger trust restoration across sectors, including nonprofit/humanitarian organizations
SCCT + topic modeling	Jechle, Schuetz & Gewald (2025)	Computational analysis of 7,900+ breach disclosures	Organizations frequently blend compensation, victimage, and apology framings simultaneously
SCCT meta-analysis	Avery & Park (2016)	Meta-analysis	Attributed responsibility significantly shapes reputational outcomes across SCCT studies
Data breach communication	Ruohonen, Hjerppe & Kortesuo (2024)	Qualitative case studies, Finland	Early communication, responsibility acceptance, apology, and authority notification distinguish successful from unsuccessful cases
Data breach communication	Masuch, Greve & Trang (2021)	Health-service provider sample	Apology and compensation strategies shape post-breach stakeholder response
Data breach communication	Schlackl, Link & Hoehle (2022)	Systematic review	Synthesizes antecedents and consequences of data breaches across the information-systems literature
Image Repair Theory	Benoit (2015)	Theoretical	Typology of denial,

			evasion, reducing offensiveness, corrective action, mortification; oriented to image protection
Trust repair	Liu & Duarte (2023)	Systematic review, health crises	Identifies recurring public-trust-repair communication mechanisms across health-crisis contexts
Nonprofit/stakeholder crisis communication	Ndlela (2019)	Theoretical/stakeholder approach	Argues crisis communication in mission-driven organizations must address a broader stakeholder set than corporate models assume
Nonprofit crisis communication	Fuller et al. (2022)	COVID-19 nonprofit sample	Corporate-derived crisis frameworks apply only partially to mission-driven organizations
Crisis communication portfolio	Nöhammer, Schorn & Becker (2023)	Conceptual	Crisis communication strategies must be optimized as a portfolio rather than a single response
Stakeholder-focused crisis case study	Marynissen & Lauder (2020)	Brussels terror-attack case study	Demonstrates stakeholder-differentiated communication strategy during an acute crisis
Humanitarian cybersecurity gap	Anfuso, Bartolucci, Del-Real & Kuipers (2026)	PRISMA-ScR scoping review	Crisis communication is identified as an underexamined dimension of humanitarian-sector cybersecurity research
Digital humanitarianism	Aradau (2023)	Critical/theoretical	Frames data collection as now central, not incidental, to humanitarian action - raising the stakes of any breach
Digital humanitarianism	Masiero (2023)	Critical discourse analysis	Documents surveillance risks associated with digitized humanitarian beneficiary systems

Digital humanitarianism	Bruder & Baar (2024)	Systematic literature review	Reviews innovation (including digital/data) trends across humanitarian assistance
Humanitarian data governance/ethics	Fast (2023)	Conceptual, humanitarian health data	Frames data governance in humanitarian delivery as a matter of relationships, trust, and ethics, not compliance alone
Humanitarian data governance/ethics	Lidén (2026)	Conceptual/governance	Examines ethical self-regulation versus stronger legal/political control of humanitarian data governance
Humanitarian information sharing	Nair, Attal-Juncqua, Reddy, Sorrell & Standley (2022)	Mixed-methods	Identifies barriers and opportunities in humanitarian health information-sharing systems
Privacy in crisis communication	Watson & Rodrigues (2017)	Conceptual	Argues privacy considerations are frequently absent from crisis-management communication research
Data-breach privacy law	Mills (2017)	Legal analysis	Frames data breaches as a mass-intrusion harm distinct from traditional privacy-tort conceptions

Source: Author's own synthesis of the sources discussed in Section 7.1; full citations appear in the References.

This review draws on 23 sources discussed above, within a reference list of ~35 verified sources. Coverage is uneven: SCCT, data-breach communication, IRT, trust repair, digital humanitarianism, and humanitarian data governance are each multiply represented; conflict-sensitive communication specifically remains unrepresented by a source

meeting this study's verification standard, and is noted as a gap rather than filled with an unverified citation.

8. Theoretical Framework

This study engages SCCT and IRT critically rather than adopting either as a predetermined lens, consistent with an inductive, theme-first coding approach. Both theories share a premise that crisis communication is strategically oriented toward image protection; SCCT calibrates response to crisis type and attributed responsibility, while IRT offers finer-grained rhetorical categories. Following the coding principle applied throughout this study, themes were allowed to emerge from the ICRC and WFP corpora before being mapped onto SCCT and IRT categories in the Discussion. Table 3 (Theoretical Construct Synthesis) below makes this mapping explicit construct-by-construct, distinguishing what each theory contributes from what neither theory was built to explain.

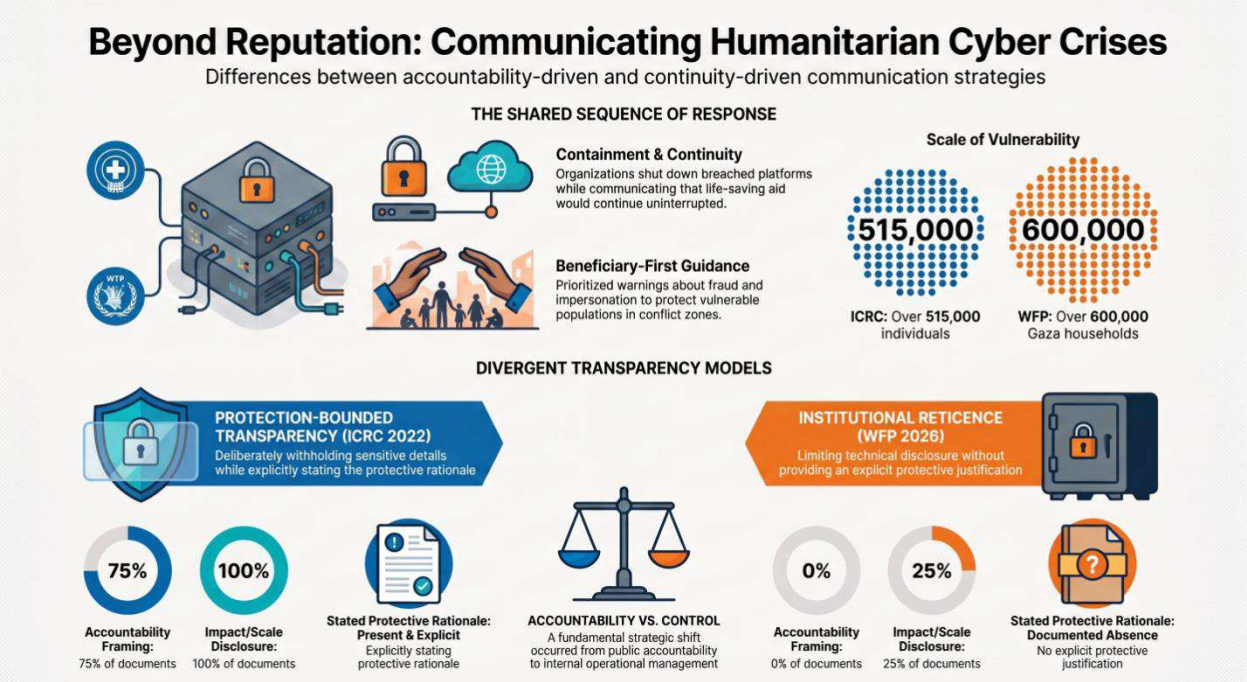


Table 3. Theoretical Construct Synthesis (SCCT, IRT, and Humanitarian Implications)

Theoretical construct	SCCT	IRT	Humanitarian implication	Evidence in corpus
Crisis responsibility / attribution	Central construct: response strategy should match attributed responsibility (victim vs. preventable crisis)	Not a central construct, though denial/evasion strategies relate to responsibility avoidance	Humanitarian organizations largely frame breaches as externally attributed ('victim') crises, but a stated pre-breach warning (WFP) complicates a purely victim framing	ICRC-01/02 (external attack framing); WFP-05/internal directive (preventability complication, secondary-sourced)
Response strategy selection	Central construct: strategy should be calibrated to crisis type	Provides finer-grained rhetorical categories (denial, evasion, reducing offensiveness, corrective action, mortification)	Neither theory specifies how strategy should be calibrated when the stakeholder is a population dependent on the organization for survival, rather than a customer or voter	ICRC-01 through 05 (multi-document strategy sequence); WFP-01 through 05 (narrower strategy range)
Corrective action	Explicitly	Explicitly	Both cases show	CoA code: ICRC

	incorporated as a response strategy	incorporated as an image-repair strategy	corrective action; humanitarian framing extends it toward beneficiary protection, not only reputational repair	4/5 documents; WFP 4/4 determinable documents
Accountability / responsibility acceptance	Partially addressed via responsibility attribution	Central construct (mortification, corrective action)	ICRC corpus shows explicit accountability language absent from the WFP corpus as currently documented	RAF code: ICRC 3/4 (75%); WFP 0/5 (0%)
Beneficiary/stakeholder protection	Not a central construct; SCCT is oriented toward organizational reputation	Not a central construct; IRT is oriented toward image protection	Neither theory was built to explain communication whose primary aim is reducing harm to a dependent population rather than protecting the organization's image	BPG code present in both corpora; motivates the study's emergent constructs rather than being explained by either theory
Disclosure-risk trade-offs	Not addressed	Not addressed	Central to this study's proposed contribution: disclosure itself may increase risk to affected populations, a consideration absent from both source theories	PBR code: ICRC 1/3 (33%) determinable, WFP 0/5 (0%); basis for protection-bounded transparency / institutional reticence constructs
Operational continuity	Not addressed	Not addressed	Humanitarian organizations must communicate about continuity of life-sustaining services, a function outside both theories' original scope	OC code: ICRC 5/5 (100%); WFP 3/4 (75%)

Source: Author's own analysis based on Coombs (2007), Benoit (2015), and the study's coding matrix (Section 12.7).

9. Methodology

This study employs a qualitative comparative content analysis, supplemented by descriptive frequency and temporal analysis where reliable timestamps are available. The unit of analysis is each discrete official communication issued by ICRC or WFP in connection with the respective breach. Sources are classified into three evidentiary levels: Level A (official organizational communication - the primary coding corpus), Level B (official UN/inter-agency documentation, used for verification), and Level C (independent media and civil-society reporting, used only for contextual triangulation, never coded as organizational communication). The study follows relevant principles of qualitative reporting transparency, drawing primarily on the Standards for Reporting Qualitative Research (SRQR); the Consolidated Criteria for Reporting Qualitative Research (COREQ) is not treated as a direct reporting standard, as the study is document-based rather than interview- or focus-group-based. As a single-coder qualitative document analysis at this stage, the study relies on an explicit codebook, an auditable evidence trail linking every code to a dated, sourced document excerpt, and negative-case attention (coding "NA" rather than "0" where a category is not evidenced, to avoid conflating absence of documentation with absence of practice) in place of a formal intercoder-reliability statistic; a second-coder reliability check (e.g., Krippendorff's alpha) is identified as a priority for the next research phase.

10. Coding Scheme

The scheme below reflects the coding categories used in the analysis. "Response interval" replaces an earlier "response speed" formulation and is calculated only where both a start and end timestamp are documented by the organization itself.

Table 4. Coding Scheme: Category Definitions

Category	Operational definition
Crisis acknowledgement	Explicit confirmation that a breach occurred.
Impact/scale disclosure	Specification of the categories and approximate volume of data/people affected.
Documented response interval	Time elapsed between two documented timestamps (e.g., detection to public disclosure); computed only where both dates are organization-confirmed.
Technical explanation	Specificity about the breach mechanism (e.g., vulnerability, attack vector).
Responsibility framing	Whether the organization frames itself as accountable, as a victim of external attack, or both.
Corrective action	Presence and specificity of remediation and hardening measures.
Beneficiary-directed protection guidance	Concrete advice to affected individuals (e.g., fraud/impersonation warnings).
Protection-bounded transparency	Explicit statement that certain details are withheld because disclosure could increase risk to affected people.
Service/mission continuity assurance	Communication addressing whether and how humanitarian assistance continues despite the incident.
Uncertainty management	Explicit distinction between what is known, unknown, and still under investigation.
Stakeholder/channel differentiation	Distinct messaging or channels for beneficiaries, donors, partners, and media.
Longitudinal follow-up	Presence of dated updates beyond the initial disclosure.

Source: Author's own codebook, developed inductively from the ICRC and WFP corpus (Section 12).

11. Verified Comparative Timeline

The table below distinguishes intrusion, detection, and disclosure as separate, non-interchangeable events, following the correction that a single undifferentiated "breach date" conflates analytically distinct moments.

Table 5. Verified Comparative Timeline (ICRC 2022 vs. WFP 2026)

Event	ICRC (2022)	WFP (2026)
Prior warning	Not documented in available corpus	Whistleblower alert to WFP's beneficiary feedback mechanism, 12 May 2026 (2 days pre-attack)
Intrusion (technical)	9 November 2021 (per ICRC's own post-incident analysis)	14 May 2026
Internal detection/confirmation	18 January 2022	14 May 2026 (same date per WFP statement; detection-vs-intrusion gap not separately specified by WFP)
First public disclosure	19 January 2022 (news release)	31 May 2026 (Telegram message; some partners/donors reportedly notified same weekend)
First direct beneficiary notification	Within initial response; expanded via FAQ/guidance pages	31 May 2026 (Telegram + email to some recipients)
Full public confirmation	19 January 2022	2 June 2026 (statement to The New Humanitarian)
Detailed technical/analytical disclosure	16 February 2022 ("Sharing our analysis"; "What we know")	Not yet documented in available official corpus
Official situation report	N/A (organization-specific formats)	9 June 2026 (WFP Palestine Emergency Response Sitrep #90)

Source: Author's own compilation from official ICRC and WFP communications and the independent sources cited in Sections 11-12 (e.g., International Committee of the Red Cross, 2022; The New Humanitarian, 2026; Access Now, 2026).

Note: The ICRC interval between detection (18 Jan) and public disclosure (19 Jan) was approximately one day; the interval between

intrusion (9 Nov 2021) and detection (18 Jan 2022) was approximately ten weeks. For WFP, detection and the attack date are reported as the same date (14 May) in available official sources; the interval most robustly documented is between the attack date and the first beneficiary notification (31 May), an interval of 17 days that has been explicitly characterized as falling short of breach-notification best practice by an independent civil-society coalition (Access Now, 2026).

12. Evidence Corpus

12.1 Source-Level Classification

Table 6. Source-Level Evidence Classification (Level A/B/C)

Source type	Example	Use in this study
Level A - Official organizational communication	ICRC news releases, open letters, FAQs; WFP Telegram notices, official statements, situation reports	Primary coding corpus
Level B - Official UN/inter-agency documentation	WFP situation report (ReliefWeb-hosted)	Verification / triangulation
Level C - Independent media and civil society	The New Humanitarian, Access Now, DataBreaches.Net, Lemkin Institute/Inklings, Al Jazeera, NPR	Contextual corroboration only - not coded as organizational communication

Source: Author's own classification scheme (Section 12.1).

12.2 ICRC - Level A Communications

Table 7. ICRC Level A Communications Included in the Corpus

Date	Document (official ICRC)	Key documented content
19 Jan 2022	Initial news release	Confirms attack on servers holding data of 515,000+ people from 60+ National Societies; states no evidence of public sharing at that time; RFL systems taken offline.

29 Jan 2022	Director-General open statement, "Hacking the data of the world's most vulnerable is an outrage"	Frames breach as an affront to humanity; names affected categories (separated families, missing persons, detainees); states data protection "is not a responsibility we have taken lightly"; references prior security investment.
~16 Feb 2022	Open letter, "ICRC cyber-attack: Sharing our analysis"	States the attack was targeted and sophisticated; describes it as exploiting an undetected vulnerability; describes low-tech continuity workarounds (e.g., spreadsheets) for RFL services; frames disclosure as an accountability obligation to partners and affected people.
~Feb 2022 (dated to detection)	"Cyber-attack on ICRC: What we know" (FAQ)	Discloses intrusion date (9 Nov 2021) and detection date (18 Jan 2022); names the exploited vulnerability (CVE-2021-40539); states no ransom demand and no contact with attackers; states technical architecture details will not be disclosed; describes server relaunch with two-factor authentication and enhanced threat detection.
Undated (post-Feb 2022)	"Cyber security incident: How could it affect me?"	Beneficiary-directed guidance; clarifies not everyone who used the services was affected; provides contact channels; confirms continuity of Restoring Family Links services.

Source: Author's own corpus compilation, drawn directly from official ICRC documents (icrc.org), as cited in Section 12.2 and the References.

12.3 WFP - Level A Communications

Table 8. WFP Level A Communications Included in the Corpus

Date	Document (official WFP)	Key documented content
31 May 2026	Telegram notification to beneficiaries (also partially via email, per independent reporting)	Describes a "security-related incident" in which "unauthorised actors" accessed personal data; specifies data categories affected (names, ID numbers, mobile numbers, location data); advises no need to re-register; warns against impersonation attempts.
2 Jun 2026	Official statement to The New Humanitarian	Confirms "unauthorized access of its self-registration application (SRA) for Palestine"; states WFP "took immediate action to shut down the platform, contain the intrusion, and strengthen its security controls."
2 Jun 2026	Follow-up Telegram message	States the application was temporarily disabled for the time needed to strengthen cybersecurity and data-protection measures (per Access Now's documented account of WFP's own message).
9 Jun 2026	WFP Palestine Emergency Response External Situation Report #90 (reporting period 1-	Official situation report confirming the incident, immediate platform shutdown, containment, security reinforcement, continuation of assistance to existing

	31 May 2026)	beneficiaries, and non-impact on other WFP systems (e.g., SCOPE).
25-29 Jul 2026	Telegram teaser message to beneficiaries ("Coming soon!!"); PDF update document addressed to partner organizations	Announces the self-registration app is restarting after unspecified 'improvements to strengthen the security of the system'; states third-party security scans were conducted and security posture strengthened; does not disclose investigation findings, a risk assessment, or the total number of people affected. This was WFP's first reply to journalist questions since 3 June 2026, indicating an approximately eight-week gap in public official communication on the incident.

Source: Author's own corpus compilation, drawn from official WFP statements as reproduced in The New Humanitarian (2026), Access Now (2026), and DataBreaches.Net (2026); see Section 12.3 and the WFP Source Verification Audit (Table 9).

Per the requirement to audit every WFP document individually rather than treat secondary-quoted material as equivalent to directly retrieved primary text, Table 9 (WFP Source Verification Audit) below classifies each WFP document's evidentiary status. Where a document is secondary-sourced, in-text language throughout this manuscript uses attributions such as 'a contemporaneous report quotes WFP as stating...' rather than an unqualified 'WFP stated...'.

Table 9. WFP Source Verification Audit

WFP document	Primary source directly retrievable?	Secondary source?	Exact quotation available?	Coding confidence
WFP-01 (31 May 2026 Telegram notification)	No - Telegram has no stable public archive page for this message	Yes - DataBreaches.Net reproduced the message text	Yes, via DataBreaches.Net's direct quotation	Moderate: wording confidence rests on one secondary outlet's quotation, not an independently verified WFP-hosted copy
WFP-02 (2 Jun 2026 statement to	No - issued as a statement to a	Yes - The New Humanitarian	Yes, via The New Humanitarian's	Moderate-High: statement was

press)	journalist, not published on a standalone WFP web page	reproduced WFP's statement	direct quotation	solicited and quoted directly by a named outlet, reducing paraphrase risk
WFP-03 (2 Jun 2026 follow-up Telegram)	No - Telegram, no stable public archive page	Yes - Access Now reproduced the message content	Yes, via Access Now's direct quotation	Moderate: single secondary source
WFP-04 (9 Jun 2026 Situation Report #90)	Yes - hosted on ReliefWeb, a stable public inter-agency archive	N/A - primary document accessible via a stable third-party archive	Partial - summarized from listing/report content rather than full verbatim retrieval of every line	Moderate-High: document itself is stably archived, but this study's excerpt is not a full verbatim pass
WFP-05 (25-29 Jul 2026 restart update)	Partial - referenced a PDF hosted at a WFP document-repository URL (docs.wfp.org), described via The New Humanitarian's reporting rather than independently fetched by this study	Yes - The New Humanitarian quoted the update directly and described the internal staff-guidance document	Yes for the quoted portions reproduced by The New Humanitarian; the underlying WFP PDF and the internal staff directive were not independently fetched by this study	Moderate: strongest WFP entry for direct quotation, but the internal directive specifically remains secondary-only evidence (see Section 12.4)

Source: Author's own source audit, cross-checking each WFP document against its retrieval method and evidentiary status (Section 12.3).

The ICRC corpus currently comprises five Level A documents spanning January-June 2022; the WFP corpus currently comprises five Level A/Level A-adjacent documents spanning 31 May-29 July 2026, none directly hosted on a stable WFP-controlled public archive comparable to icrc.org. This asymmetry in corpus size, time span, and source stability is treated as a documented feature of the comparison, not concealed, and is addressed directly in Section 16 (Limitations).

12.4 A Note on Internal Communication Guidance (WFP)

Independent reporting on 29 July 2026 disclosed the content of an internal WFP frontline-staff guidance document, prepared in connection with the self-registration app's relaunch, instructing staff: do not provide technical explanations about previous security incidents unless directed by approved WFP messaging, and to focus instead on improvements and current access (The New Humanitarian, 2026, 29 July). This is not a public communication and is therefore coded separately from the Level A corpus above, but it is treated as directly relevant evidence of organizational communication strategy, since it documents an explicit internal instruction to limit disclosure. Unlike the ICRC corpus, in which limited disclosure is accompanied by an explicit, stated protection rationale (Section 12.2), no equivalent public rationale for limiting disclosure has been identified in the WFP corpus; external stakeholders, including the digital rights organization Access Now, have explicitly characterized this absence of explanation as unjustified rather than protective (The New Humanitarian, 2026, 29 July).

12.5 Master Corpus Table

The full master corpus table, listing every document considered for inclusion (ID, organization, date, platform, type, and inclusion rationale), is provided as Supplementary Table S1.

12.6 Codebook

The full codebook, giving the operational definition, inclusion rule, and exclusion rule for each of the twelve codes, is provided as Supplementary Table S2 (a condensed version of the operational definitions appears above in Table 4).

12.7 Master Coding Matrix

Each document was coded 1 (clearly present), 0 (clearly absent), or NR (not reliably determinable from the primary text currently retrieved); ambiguous evidence was not forced into 0 or 1. The full document-by-document coding matrices for ICRC and WFP are provided as Supplementary Tables S3 and S4.

12.8 Frequencies

Percentages below are calculated only across documents for which a given code was determinable (denominator shown), following Step 5: percentage = (documents coded 1 / total determinable documents) x 100. Given denominators of 2-5 documents per case, these frequencies are descriptive of the current corpus only and are not statistically generalizable; they are reported to make the analysis auditable, not to imply population-level inference.

Table 10. Coding Frequencies by Organization

Code	ICRC (n present/n determinable, %)	WFP (n present/n determinable, %)
CA	5/5 (100%)	5/5 (100%)
ISD	5/5 (100%)	1/4 (25%)
TE	2/5 (40%)	0/5 (0%)
RAF	3/4 (75%)	0/5 (0%)
CoA	4/5 (80%)	4/4 (100%)
EMP	5/5 (100%)	0/4 (0%)
BPG	2/4 (50%)	1/4 (25%)
PBR	1/3 (33%)	0/5 (0%)
OC	5/5 (100%)	3/4 (75%)
TOC	2/4 (50%)	0/5 (0%)
FP	5/5 (100%)	4/5 (80%)
UM	3/4 (75%)	0/2 (0%)

Source: Author's own calculation from the Master Coding Matrix (Supplementary Tables S3-S4); percentages are descriptive corpus-level frequencies, not inferential statistics (Section 12.8).

Figure 1 visualizes this comparison for codes with at least three determinable documents per case (excluding TE, BPG, PBR, TOC, and UM for WFP or ICRC where the determinable count falls below this threshold, to avoid over-interpreting very small denominators).

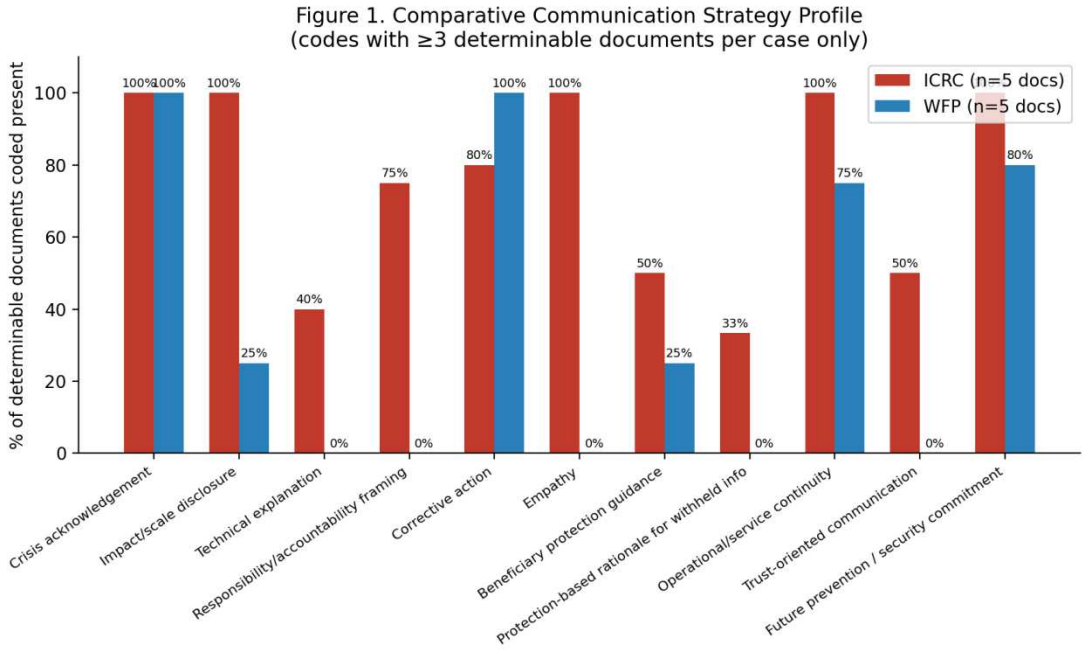


Figure 1. Comparative Communication Strategy Profile. Bars show the percentage of determinable documents per organization coded present for each dimension; exact fractions are in Section 12.8.

12.9 Timeline Figure

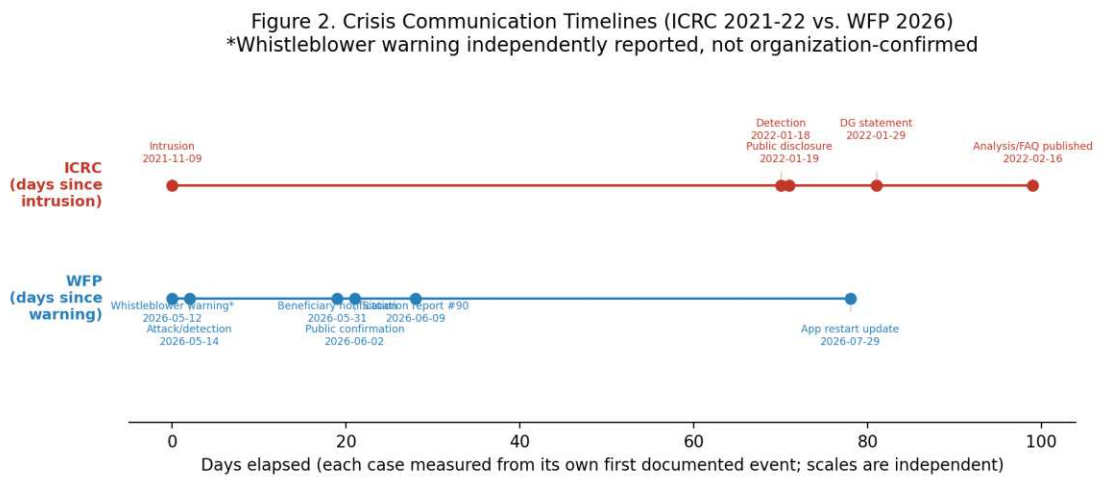


Figure 2. Crisis Communication Timelines. Each organization's events are plotted as days elapsed from its own first documented event (independent scales); no missing dates were inferred.

13. Findings

13.1 ICRC

Across its five Level A communications, the ICRC corpus documents a sustained sequence moving from acknowledgement (19 Jan) to explicit institutional accountability framing (29 Jan: "this is not a responsibility we have taken lightly") to detailed technical and analytical disclosure (~16 Feb: intrusion date, exploited vulnerability, remediation measures) to beneficiary-directed guidance. Two features recur across multiple documents: first, an explicit accountability framing that credits ICRC's obligation to "partners and the people we serve"; second, an explicit and repeated statement that certain details - for instance, regarding the identity or location of individuals - are not disclosed because doing so

would not serve affected people's interests. This second feature is coded as protection-bounded transparency: transparency exercised for accountability purposes but deliberately bounded where further disclosure could itself cause harm.

13.2 WFP

Across its five currently documented Level A communications, spanning 31 May to 29 July 2026, the WFP corpus shows a consistent emphasis on beneficiary notification, protective/anti-fraud guidance, incident containment, security-control reinforcement, and - distinctively - assurance that humanitarian assistance to existing beneficiaries continues uninterrupted despite the platform shutdown. Institutional responsibility framing is present but less developed than in the ICRC corpus: WFP's official statements center on "unauthorized access" and remediation steps rather than on an extended accountability narrative, and no risk assessment, investigation findings, or confirmed total-affected figure had been publicly disclosed as of the most recent documented communication. This pattern is no longer attributable only to case recency: the corpus now documents an approximately eight-week gap in public communication (2 June-29 July 2026) and an internal staff-guidance instruction to limit technical explanation of the incident (Section 12.4), both of which are consistent with an emphasis on operational continuity and controlled messaging rather than extended

public accountability; the interpretive significance of this pattern is addressed in the Discussion (Section 14).

13.3 Cross-Case Comparison

Table 11. Cross-Case Comparison of Coding Dimensions

Coding dimension	ICRC	WFP	Interpretation (preliminary)
Crisis acknowledgement	1	1	Present in both cases
Impact/scale disclosure	1	1	Present in both cases
Detailed technical explanation	1	NA	More developed in ICRC's available corpus
Explicit institutional responsibility framing	1	NA	More explicit in ICRC's available corpus
Corrective action (containment, hardening)	1	1	Present in both cases
Beneficiary-directed protective guidance	1	1	Present in both cases
Direct beneficiary notification channel	1	1	ICRC: multi-channel outreach; WFP: Telegram/email
Service/mission continuity assurance	1	1	Central to both cases
Protection-based limits on disclosure	1	NA	Explicitly documented for ICRC; not yet evidenced for WFP
Anti-fraud/impersonation guidance	NA	1	More explicit in WFP's available corpus
Extended longitudinal follow-up	1	1 (with an ~8-week gap, 2 Jun-29 Jul)	Both now span multiple months; WFP shows a documented silence interval
Explicit protection rationale for withheld disclosure	1	0	ICRC states a rationale for non-disclosure; internal WFP guidance instructs staff to avoid technical explanation without stating a protective rationale, and this omission is explicitly criticized by external stakeholders

Source: Author's own analysis based on the Master Coding Matrix (Supplementary Tables S3-S4) and Evidence Corpus (Tables 7-8).

The comparative evidence indicates that both organizations employed a shared core sequence - acknowledgement, containment, corrective action, beneficiary guidance, and continuity assurance - while differing in dominant orientation and in the treatment of disclosure limits specifically. The two cases suggest an accountability- and explanation-centered pattern in the ICRC corpus, paired with an explicitly justified boundary on disclosure, and a continuity- and control-centered pattern in the WFP corpus, in which disclosure limits are documented but not accompanied by a stated protective rationale and have been explicitly contested by external stakeholders as unjustified. This distinction is now grounded in nine weeks of WFP corpus observation (31 May-29 July 2026) rather than an initial nine-day window, and is treated as a provisional finding pending closure of the full corpus.

14. Discussion



The findings offer partial support for SCCT's premise that organizations facing an externally attributed crisis favor disclosure paired with reassurance over denial - both organizations disclosed rather than concealed, and neither employed denial strategies in the available corpus. However, the humanitarian context surfaces a pattern not well captured by SCCT or IRT in their original corporate formulations. Where SCCT treats disclosure primarily as a lever for reputation management, the ICRC corpus demonstrates disclosure being explicitly and repeatedly weighed against a distinct risk: that disclosure itself may endanger the very population the disclosure is meant to inform, with the organization stating this rationale directly. This pattern is provisionally termed protection-bounded transparency: limited disclosure justified openly, in terms the organization itself articulates.

The WFP corpus, once extended to 29 July 2026, documents a related but analytically distinct pattern. As an empirical observation: WFP also limits disclosure - it has not published investigation findings, a risk assessment, or a confirmed total-affected figure - but, unlike ICRC, no document in the corpus articulates a protective rationale for these limits; internal guidance instead directs staff toward messaging about improvements rather than explanation, and external stakeholders have explicitly rejected the possibility of a protective justification (per Access Now's senior humanitarian officer, as reported by The New Humanitarian, 2026, 29 July, who is quoted stating that no justification for the lack of transparency exists). This observed pattern - limited disclosure without an explicitly documented protective rationale - is interpreted here as institutional reticence. This label is a researcher interpretation of the pattern, not a claim about WFP's internal motives or intent, which this study's document-based design cannot establish; the corpus supports the observation that a rationale is absent from the public record, not a conclusion about why it is absent. The distinction between protection-bounded transparency and institutional reticence is offered as this study's central comparative contribution: both are compatible with SCCT's general expectation that organizations avoid denial, but only the former is documented as being tied to a stated beneficiary-protection purpose. Whether this distinction generalizes beyond these two cases cannot yet be established from a two-case design; testing it against

additional humanitarian-sector breaches, as they are documented, is identified as a specific next step.

A second candidate theme is humanitarian operational continuity communication: in both cases, but especially in WFP's currently documented corpus, a substantial share of crisis communication is directed not at reputation management but at reassuring beneficiaries that essential assistance continues despite the incident. This suggests that, in humanitarian settings, crisis communication may serve risk-mitigation and service-continuity functions that sit outside the reputation-centered logic of SCCT and IRT as originally formulated.

15. Proposed Framework: Humanitarian Cyber Crisis Communication and Protection Framework (HCCCPF)

Building on the findings above, a six-phase, cyclical framework is proposed, organized around a central Protection Boundary construct: at each phase, the organization must assess whether a given disclosure could increase the risk of harm to affected populations, and calibrate transparency accordingly. This reframes limited disclosure not as a transparency deficit but as a deliberate, justifiable communicative choice under a distinct set of humanitarian obligations.

Table 12. HCCCPF Phase Structure

Phase	Principle	Core actions	Beneficiary need addressed	Theoretical basis
0. Pre-Crisis	Preparedness	Cyber-risk mapping; data minimization; pre-drafted	Reduced likelihood/impact of	SCCT (situational preparedness)

		notification protocols; stakeholder mapping	future exposure	
1. Detection	Verify & assess	Confirm breach; scope affected systems and populations; assess humanitarian risk of disclosure itself	Accurate basis for any communication that follows	Risk/crisis communication literature
2. Initial Response	Acknowledge & protect	Acknowledge incident; communicate verified facts; issue protective guidance; counter misinformation/impersonation	Knowing whether one is affected and what to do	SCCT; humanitarian data-protection guidance
3. Accountability	Explain & act within the Protection Boundary	Explain what is known and not yet known; accept institutional responsibility where appropriate; describe corrective measures; where details are withheld, state the protective rationale explicitly (distinguishing protection-bounded transparency from unexplained institutional reticence)	Trust that the organization is accountable without further exposure	IRT (accountability strategies); emergent themes: Protection-Bounded Transparency vs. Institutional Reticence
4. Continuity & Trust	Protect the mission	Reassure on continuity of assistance; restore systems; sustain stakeholder communication; reduce uncertainty	Confidence that aid will continue	Emergent theme: Humanitarian Operational Continuity
5. Recovery & Resilience	Learn & improve	Independent review; technical and policy reform; transparent lessons-learned communication; feed forward into Phase 0	Confidence that recurrence is being addressed	Organizational learning literature; feeds back to Phase 0

Source: Author's own framework synthesis, derived from the findings in Section 13 and the theoretical framework in Section 8.

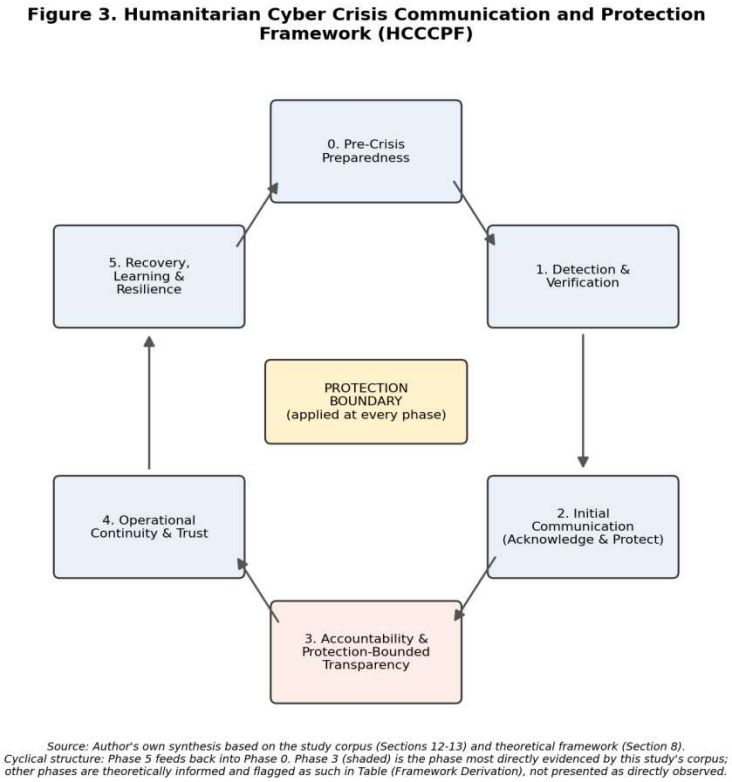


Figure 3. Humanitarian Cyber Crisis Communication and Protection Framework (HCCCPF). The six-phase cyclical framework, with the Protection Boundary construct applied at every phase; Phase 3 (shaded) is the phase most directly evidenced by this study's corpus.

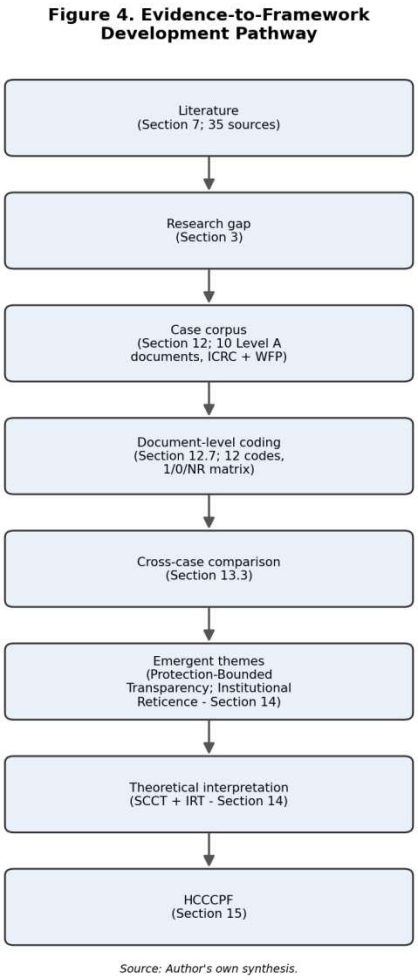


Figure 4. Evidence-to-Framework Development Pathway. The developmental path from the literature review through case-corpus coding and cross-case comparison to the proposed HCCCPF.

Table 13 (Framework Derivation) below traces each HCCCPF component to the specific documents, codes, and theoretical basis that support it, distinguishing components that are directly evidenced from those that remain theoretically informed recommendations.

Table 13. Evidence-to-HCCCPF Derivation

Framework component	Empirical evidence	Case(s)	Coding categorie	Theoretical basis	Status

			s		
0. Pre-Crisis Preparedness	Neither corpus documents pre-breach preparedness communication directly (by definition, preparedness precedes public communication)	N/A	N/A	SCCT (situational readiness); general crisis-management literature (Ndlela, 2019)	Theoretically informed recommendation, not directly evidenced
1. Detection & Verification	ICRC explicitly dates detection (18 Jan 2022) separately from intrusion (9 Nov 2021); WFP dates detection/attack to 14 May 2026	ICRC-04; WFP-02, WFP-04	CA, UM	Risk/crisis communication literature (Ruohonen et al., 2024)	Empirically evidenced (ICRC); partially evidenced (WFP)
2. Initial Communication (Acknowledge & Protect)	Both corpora show acknowledgement in the first public communication, paired with beneficiary-directed guidance	ICRC-01, ICRC-05; WFP-01	CA, BPG	SCCT (initial response strategy)	Empirically evidenced in both cases
3. Accountability & Protection-Bounded Transparency	ICRC states an explicit accountability rationale (ICRC-03: 'responsibility...accountable to our partners and the people we serve') and an explicit protection-based non-disclosure rationale (ICRC-04); WFP's internal guidance limits explanation without a stated rationale (Section 12.4)	ICRC-03, ICRC-04; WFP internal directive (via TNH, 29 Jul 2026)	RAF, PBR, TE	IRT (accountability strategies); emergent constructs: Protection-Bounded Transparency, Institutional Reticence	Most directly evidenced phase in the corpus
4. Operational Continuity & Trust	Both corpora contain explicit continuity-of-assistance statements	ICRC-01, ICRC-02, ICRC-05; WFP-01, WFP-04, WFP-05	OC, TOC	Emergent theme: Humanitarian Operational Continuity	Empirically evidenced in both cases
5. Recovery,	ICRC documents security	ICRC-	FP	Organizational	Partially

Learning & Resilience	hardening and relaunch with enhancements (ICRC-04); WFP documents an app restart with strengthened security posture but no published lessons-learned document (WFP-05)	04; WFP-05		learning literature (general)	evidenced; 'lessons-learned' publication not observed for either case within the corpus window

Source: Author's own derivation table, tracing each framework component to its supporting documents, codes, and theoretical basis (Section 15).

Unlike a purely linear pre-crisis/immediate/advanced/post-crisis timeline, this framework is cyclical: Phase 5 (Recovery & Resilience) feeds directly back into Phase 0 (Pre-Crisis), reflecting that organizational learning from one incident should inform preparedness for the next. The framework is offered as conceptually promising but empirically preliminary: it is grounded in the ICRC corpus more fully than the WFP corpus at this stage, and each phase requires further justification once both corpora are closed and coded to completion.

16. Limitations

This study has several limitations. First, it remains a two-case design with documentary data only; it does not include interview or audience-reception data, and therefore cannot support causal claims about actual trust restoration, only about the communicative strategies organizations employed. Second, a temporal asymmetry remains, though it has narrowed: the ICRC corpus spans roughly five months of documented communication (January-June 2022), while the WFP corpus now spans

roughly nine weeks (31 May-29 July 2026), and the true size of the eventual WFP corpus is not yet known, since the underlying incident and its aftermath remain current at the time of writing. Third, coding to date has been conducted by a single researcher; a second-coder reliability check has not yet been performed and is identified as a priority next step rather than a completed safeguard. Fourth, both cases occurred within active-conflict or conflict-adjacent settings, which may limit generalizability to humanitarian data breaches in non-conflict contexts. Fifth, the internal WFP staff-guidance document discussed in Section 12.4 was not published by WFP itself but disclosed through independent journalism; its authenticity rests on that reporting rather than on direct organizational confirmation.

Sixth, on data transparency: all factual claims are drawn from officially verified sources (References); no citation, date, or figure has been invented, though three items remain open: (1) the exact publication date of ICRC's beneficiary-facing "How could it affect me?" guidance has not been independently confirmed from source metadata and is marked accordingly in Section 12.2; (2) the WFP pre-breach whistleblower warning (12 May 2026) is corroborated by two independent sources (reporting citing The New Humanitarian, and the Lemkin Institute/Inklings account) but has not been confirmed in WFP's own official communications and should be treated as independently reported rather than organization-confirmed; (3) the internal WFP staff-guidance

document discussed in Section 12.4 is known to this study only through The New Humanitarian's 29 July 2026 reporting, not through direct access to the document itself, and should be attributed accordingly; (4) coding scores in Sections 12-13 reflect single-coder qualitative judgment against an explicit evidence trail, not a validated multi-coder measurement, and should be read accordingly.

17. Future Research Directions

Priority next steps include: (1) closing both corpora through systematic, dated collection of all subsequent official communications; (2) conducting a second-coder reliability check (e.g., Krippendorff's alpha) on a sample of the coded corpus; (3) testing whether protection-bounded transparency and humanitarian operational continuity communication generalize to additional humanitarian-sector breaches as they are documented; and (4) empirically testing the HCCCPF through practitioner interviews or organizational document analysis, which would also allow more direct application of interview-based reporting standards (e.g., COREQ) than the current document-based design permits.

18. Conclusion

This paper presents an evidence-grounded research design, a source-verified comparative timeline, an evidence-linked coding scheme, and preliminary findings on crisis communication following data breaches at

two major humanitarian organizations. Both cases are independently documented, though the WFP corpus remains substantially smaller and more recent than the ICRC corpus at the time of writing. The findings, while preliminary, identify two candidate contributions - protection-bounded transparency and humanitarian operational continuity communication - that are not well accounted for in corporate-derived frameworks such as SCCT and IRT. The proposed Humanitarian Cyber Crisis Communication and Protection Framework (HCCCPF) is offered as a preliminary, evidence-grounded framework requiring validation across additional humanitarian cyber-crisis cases, not as a finished or externally validated model. This study analyzes organizational communication strategies rather than measuring audience trust outcomes directly; no claim is made that either organization's communication restored public trust, only that specific communications were oriented toward trust repair.

Declarations

Ethics approval and consent to participate

This research did not involve human participants, human data, or animal subjects, and did not require approval from an institutional ethics review board. All data analyzed were drawn from publicly available official communications and documents issued by the organizations studied, or from independently published secondary reporting of such communications.

Consent for publication

Not applicable. This study did not involve any individual person's data, images, or other personal material requiring consent for publication.

Availability of data and materials

The documentary corpus analyzed in this study consists of publicly available official communications issued by the International Committee of the Red Cross (ICRC) and the World Food Programme (WFP), together with independently published secondary reporting, all of which are cited in the References. The Master Corpus Table, Codebook, and Coding Matrix compiled by the authors are available as Supplementary Information or from the corresponding author upon reasonable request.

Competing interests

The authors declare that they have no competing interests.

Funding

[PLEASE CONFIRM: e.g., “This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.” OR insert actual funding source/grant number.]

Authors' contributions

[PLEASE CONFIRM CONTRIBUTIONS – SUGGESTED TEXT:] Ibrahim Ukka supervised the study, contributed to the theoretical framing, and critically reviewed the manuscript. Duha Najeh Mazeed and Aya Mohammad Riyad Hawash conducted the data collection, coding, and analysis, and drafted the manuscript. Febriansyah Putra

Djaya Indra contributed part of the theoretical framework. All authors read and approved the final manuscript.

Acknowledgements
[NOT APPLICABLE / INSERT TEXT IF ANY.]

References

Access Now. (2026, June 18). Surveilled, targeted, and now hacked: WFP must protect Palestinians in Gaza after massive data breach [Press release]. https://www.accessnow.org/press-release/wfp-palestinians-data-breach/

Al Jazeera. (2022, January 20). Cyberattack on ICRC exposes data on 515,000 vulnerable people. https://www.aljazeera.com/news/2022/1/20/cyberattack-on-icrc-exposes-data-on-515000-vulnerable-people

Anfuso, C., Bartolucci, A., Del-Real, C., & Kuipers, S. (2026). Cybersecurity threats, challenges, and strategies in humanitarian operations: A scoping review. International Journal of Disaster Risk Reduction. https://www.sciencedirect.com/science/article/pii/S2212420926000944

Aradau, C. (2023). The tangle of digital humanitarianism. London Review of International Law, 11(3), 523-534. https://doi.org/10.1093/lril/lrae004

Avery, E. J., & Park, S. (2016). Effects of attributed responsibility and response strategies on organizational reputation: A meta-analysis of situational crisis communication theory research. Journal of Public Relations Research, 28(2), 102-119. https://doi.org/10.1080/1062726X.2016.1166367

Benoit, W. L. (2015). Accounts, excuses, and apologies: Image repair theory and research (2nd ed.). SUNY Press.

Bruder, M., & Baar, T. (2024). Innovation in humanitarian assistance - a systematic literature review. Journal of International Humanitarian Action, 9(1), 2. https://doi.org/10.1186/s41018-023-00144-3

Choi, J., Robinson, S., Ruddle, T., & Fister, A. (2025). Restoring public trust after a data breach crisis: Reputational response strategies for government, for-profit, and nonprofit organizations. Risk, Hazards & Crisis in Public Policy, 16, e70026. https://doi.org/10.1002/rhc3.70026

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. Corporate Reputation Review, 10(3), 163-176.

DataBreaches.Net. (2026, June 2). Data of 600,000 Gaza households exposed in World Food Programme cyberattack. https://databreaches.net/2026/06/02/data-of-600000-gaza-households-exposed-in-world-food-programme-cyberattack/

Fast, L. (2023). Governing data: Relationships, trust, and ethics in leveraging data and technology in service of humanitarian health delivery. Daedalus, 152(3), 125-140.

Fuller, R. P., et al. (2022). Nonprofit organization communication, crisis planning, and strategic responses to the COVID-19 pandemic. Journal of Philanthropy and Marketing, e1750. https://doi.org/10.1002/nvsm.1750

International Committee of the Red Cross. (2022, January 19). Cyber-attack on the ICRC: What we know [News release]. https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people

International Committee of the Red Cross. (2022, February). Cyber-attack on ICRC: What we know [FAQ]. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

International Committee of the Red Cross. (2022). Cyber security incident: How could it affect me? https://www.icrc.org/en/document/cyber-security-how-it-affect-me

International Committee of the Red Cross. (2022, February 16). ICRC cyber-attack: Sharing our analysis [Open letter]. https://www.icrc.org/en/document/icrc-cyber-attack-analysis

Jechle, D., Schuetz, S., & Gewald, H. (2025). Decoding data breach response strategies: Insights from situational crisis communication theory using topic modeling. Proceedings of the European Conference on Information Systems (ECIS 2025). https://aisel.aisnet.org/ecis2025/security/security/2/

Kuipers, S., & Schonheit, M. (2022). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. Corporate Reputation Review, 25(3), 176-197. https://doi.org/10.1057/s41299-021-00121-9

Kuipers, S., Perlstein, S., Wolbers, J., & Jong, W. (2023). Assist or accuse? Identifying trends in crisis communication through a bibliometric literature review. Risk, Hazards & Crisis in Public Policy, 14(4), 272-296. https://doi.org/10.1002/rhc3.12283

Lemkin Institute / Inklings. (2026, June 3). WFP cyber-attack: Is nearly all of Gaza's population exposed? https://www.lemkininstitute.com/single-post/wfp-cyber-attack-is-nearly-all-of-gaza-s-population-exposed-the-food-programme-is-often-seen-to-be

Lidén, K. (2026). Ethics and the governance of digital data in humanitarian action. Disasters. https://doi.org/10.1111/disa.70018

Liu, Y., & Duarte, H. (2023). Repairing public trust through communication in health crises: A systematic review of the literature. Public Management Review. https://doi.org/10.1080/14719037.2023.2284224

Mardini, R. (2022, January 29). Hacking the data of the world's most vulnerable is an outrage. International Committee of the Red Cross. https://www.icrc.org/en/document/hacking-data-outrage

Marynissen, H., & Lauder, M. (2020). Stakeholder-focused communication strategy during crisis: A case study based on the Brussels terror attacks. International Journal of Business Communication, 57(2), 176-193.

Masiero, S. (2023). Digital humanitarianism: A critical discourse analysis. Proceedings of the 15th Mediterranean Conference on Information Systems / 6th MENACIS.

Masuch, K., Greve, M., & Trang, S. (2021). What to do after a data breach? Examining apology and compensation as response strategies for health service providers. Electronic Markets, 31, 829-848.

Mills, J. L. (2017). Privacy, mass intrusion, and the modern data breach. Florida Law Review, 69(3), 771-830.

Nair, S., Attal-Juncqua, A., Reddy, A., Sorrell, E. M., & Standley, C. J. (2022). Assessing barriers, opportunities and future directions in health information sharing in humanitarian contexts: A mixed-method study. BMJ Open, 12(4).

Ndlela, M. N. (2019). Crisis communication: A stakeholder approach. Palgrave Macmillan.

Nöhammer, E., Schorn, R., & Becker, N. (2023). Optimizing the organizational crisis communication portfolio. Corporate Reputation Review, 26, 304-319.

Ruohonen, J., Hjerppe, K., & Kortesuo, K. (2024). Crisis communication in the face of data breaches. arXiv:2406.01744. https://arxiv.org/abs/2406.01744

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. Information & Management, 59(4), 103638.

The New Humanitarian. (2026, June 2). Data of 600,000 Gaza households exposed in WFP cyber-attack. https://www.thenewhumanitarian.org/news/2026/06/02/data-600000-gaza-households-exposed-wfp-cyber-attack

The New Humanitarian. (2026, July 29). WFP restarts Gaza aid registration app, but cyber-attack questions linger. https://www.thenewhumanitarian.org/news/2026/07/29/wfp-restarts-gaza-aid-registration-app-cyber-attack-questions-linger

Watson, H., & Rodrigues, R. (2017). Bringing privacy into the fold: Considerations for the use of social media in crisis management. Journal of Contingencies and Crisis Management, 26, 89-98.

WFP Palestine Emergency Response External Situation Report #90 (9 June 2026, reporting period 1-31 May 2026). ReliefWeb. https://reliefweb.int/report/occupied-palestinian-territory/wfp-palestine-emergency-response-external-situation-report-90-9-june-2026-reporting-period-1-31-may-2026

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- TablesOnlyCyberCrisisCommunication1.docx
- tabels.docx
- SupplementaryInformation.docx