OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

GUIDANCE NOTE SERIES
DATA RESPONSIBILITY IN HUMANITARIAN ACTION

NOTE #2: DATA INCIDENT MANAGEMENT

KEY TAKEAWAYS:

- Humanitarian data incidents are events involving the management of data that have caused harm or have the potential to cause harm to crisis-affected people, organizations and their operations, and other individuals or groups.
- Examples of humanitarian data incidents include physical breaches of infrastructure, unauthorised disclosure of data, and the use of beneficiary data for non-humanitarian purposes, among others.
- A data incident has four aspects: (i) a threat source, (ii) a threat event, (iii) a vulnerability and (iv) an adverse impact.
- There are five steps to responding to data incidents: (i) notification, (ii) classification, (iii) treatment, and (iv) closure of the incident, as well as (v) learning.

WHAT IS A DATA INCIDENT IN HUMANITARIAN RESPONSE?

In the humanitarian sector, data incidents are events involving the management of data that have caused harm or have the potential to cause harm to crisis affected populations, humanitarian organisations and their operations, and other individuals or groups. These events can exploit or exacerbate existing vulnerabilities.[1] In some cases, they may also create new vulnerabilities that can increase the risk of future data incidents.

Humanitarians have not had a common understanding of what comprises a data incident, nor is there a minimum technical standard for how these incidents should be prevented and managed. How the humanitarian sector develops tools and implements procedures for data incident management will play a significant role in the evolution of the ethical, human rights, technical, and professional standards of humanitarian operations.

> "If aid actors digitize more of their data and communications, they urgently need to increase their digital security efforts. Though some actors are developing promising protective tools, aid organizations overall might be well advised to listen to a quote from IT-security circles: 'There are two types of organizations: those who have been hacked, and those who will be."
>
> - Rahel Dette, Do No Digital Harm: Mitigating Technology Risk in Humanitarian Contexts

[1] "A *vulnerability* is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source." **NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments**.

Humanitarian data incidents may include physical breaches of infrastructure, unauthorised disclosure of data, and the use of 'anonymised' beneficiary data for non-humanitarian purposes, among others. Data incidents can also occur without technical infrastructure being compromised in any way. The legitimate collection, use, and sharing of data by humanitarians can still have operational implications that may constitute a data incident in cases where rumors, cultural sensitivities, political dynamics, and other factors lead to adverse effects linked to the data.

DEFINITIONS AND FRAMEWORKS FOR UNDERSTANDING DATA INCIDENTS

Governments and the private sector have developed definitions and frameworks for understanding data incidents that serve as helpful references for the humanitarian sector.

- The International Organization for Standardization's (ISO) in *ISO Standard 27000* defines a 'critical incident' as "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security."[2]

- The United States Department of Commerce National Institute for Standards and Technology (NIST) defines an adverse event involving a 'cyber threat' as "[a]n event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss."[3]

- Mahmood Sher-Jan of the International Association of Privacy Professionals (IAPP) identifies three additional categories of events that expand upon the NIST definition of adverse events. These are, in order of escalating severity: security incidents; privacy incidents; and data breaches.[4]

Examples of possible humanitarian data incidents

A data incident has four factors: a threat source, a threat event, a vulnerability and an adverse impact.[5] Below are two types of hypothetical data incidents that could occur in humanitarian contexts.

The first scenario is a typical data breach incident situated in the context of an armed conflict. The second is an example of the type of vulnerabilities that can initiate data incidents unique to the humanitarian sector.

1. Unauthorized access to data occurs **[impact]** due to armed actors **[source]** raiding a facility and seizing hard-drives containing beneficiary data **[event]**. The hard-drives were unencrypted **[vulnerability]**.

2. Absence of guidance limiting data collection for a specific purpose **[vulnerability]** leads to staff collecting data about the marital status of pregnant women **[source]**. A data breach **[event]** later occurs, resulting in an increased chance of physical violence **[impact]** against unwed pregnant beneficiaries.

These scenarios demonstrate how to think about identifying causal chains that may create context-specific data incidents.

[2] International Organization for Standardization, ISO/IEC 27000:2018.

[3] NIST Computer Security Resource Center Glossary.

[4] IAPP, Is It an Incident or a Breach, How to Tell and Why It Matters, Mahmoud Sher-Jan (February 2017).

[5] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

RISK MODELS

The figure below presents a generic risk model with risk factors that organizations can use to understand how a data incident may occur. A threat event exploits an existing vulnerability that is either magnified by predisposing conditions or mitigated by security controls already in place. This causes adverse impacts that produce organizational risk, which can include risks for the organization and for affected people.

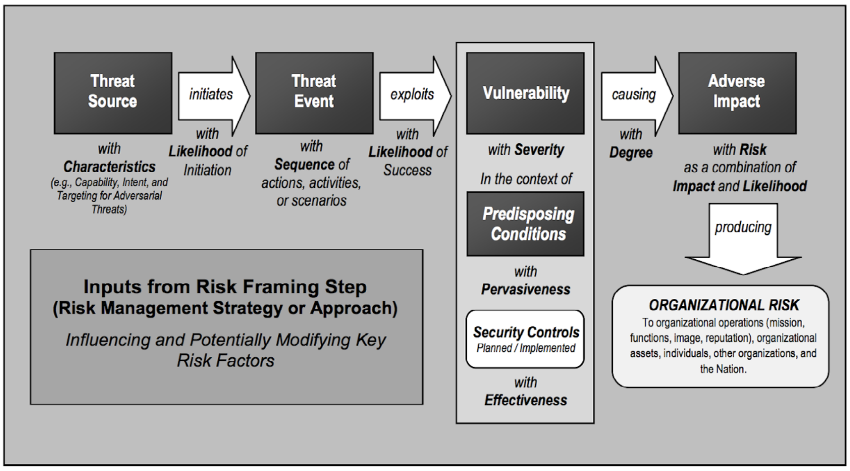
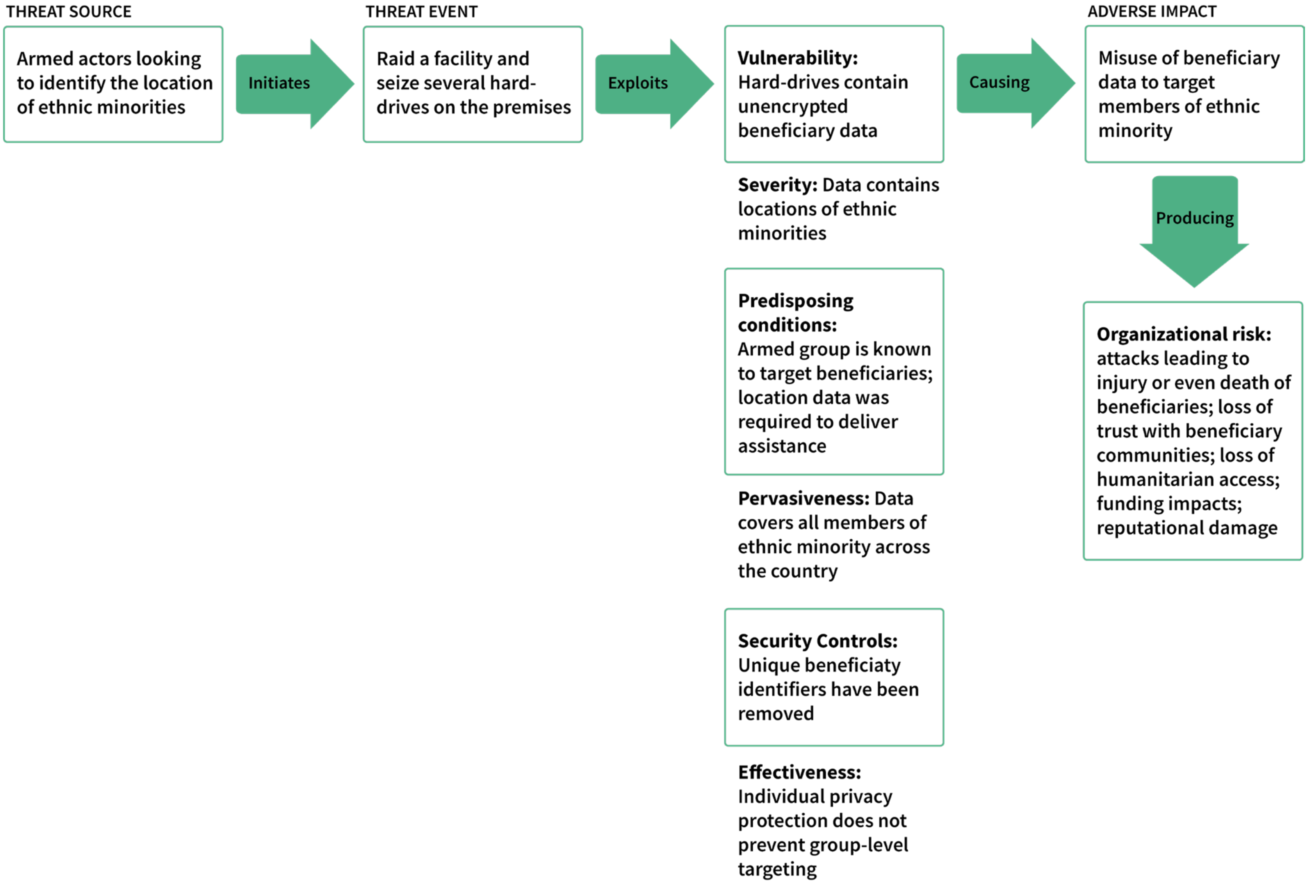

Threat Source
initiates
Threat Event
exploits
Vulnerability
causing
Adverse Impact
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
with Likelihood of Initiation
with Sequence of actions, activities, or scenarios
with Likelihood of Success
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned / Implemented
with Effectiveness
with Degree
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step (Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

Figure 1. “Generic Risk Model with Key Risk Factors”. Source: NIST Special Publication 800-30 pg. 12[6]

The figure below presents one example of how this generic risk model could be adapted to the humanitarian sector.



THREAT SOURCE

Armed actors looking to identify the location of ethnic minorities

Initiates

THREAT EVENT

Raid a facility and seize several hard-drives on the premises

Exploits

Vulnerability: Hard-drives contain unencrypted beneficiary data

Severity: Data contains locations of ethnic minorities

Predisposing conditions: Armed group is known to target beneficiaries; location data was required to deliver assistance

Pervasiveness: Data covers all members of ethnic minority across the country

Security Controls: Unique beneficiaty identifiers have been removed

Effectiveness: Individual privacy protection does not prevent group-level targeting

Causing

ADVERSE IMPACT

Misuse of beneficiary data to target members of ethnic minority

Producing

Organizational risk: attacks leading to injury or even death of beneficiaries; loss of trust with beneficiary communities; loss of humanitarian access; funding impacts; reputational damage

Figure 2. Risk Model with Key Risk Factors adapted to a humanitarian context.

[6] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

Humanitarian organizations can develop their own specific risk models for data incident management incorporating these factors. The nature of these risk factors and how they come together to constitute a data incident will vary from one organization to another and should be adapted to specific operational realities.

STEPS IN DATA INCIDENT MANAGEMENT

After clearly defining what constitutes a data incident, organizations can develop Standard Operating Procedures (SOPs) for data incident management.

Data incident management SOPs should include the following 5 steps: 1) notification, 2) classification; 3) treatment; 4) closure; and 5) knowledge base.[7]

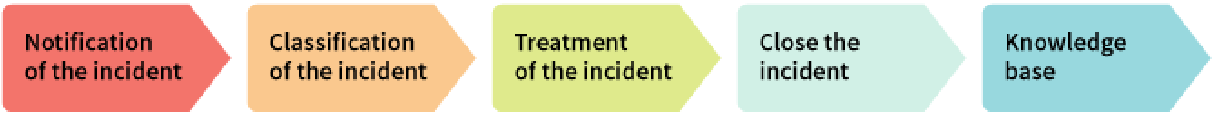

Notification of the incident
Classification of the incident
Treatment of the incident
Close the incident
Knowledge base

Figure 3: Five steps in the treatment of security incidents (Source: *How to handle incidents according to ISO 27001 A.16, Antonio Jose Segovia*[8]

The application of these steps in an organization can look as follows:

1. **Notification of the incident**: A person detects an incident and notifies relevant colleagues according to the communication procedures of the organization (usually an email, a phone call, a software tool, etc.). A notification should contain, if possible, a description of the key risk factors involved in the incident: source, event, vulnerability and impact.

2. **Classification of the incident**: The recipient of the notification classifies the incident based on it's impact (high, medium or low) and the urgency of treatment (high, medium or low).[9] Managing risk begins with classifying all incidents, whether or not tangible harm actually results from them.[10]

3. **Treatment of the incident**: A technical expert decides on the necessary measures to treat the incident once the incident has been classified and the time for treatment has been agreed.

4. **Closure of the incident**: All information generated during the treatment is recorded and the person who first sent notification of the incident is informed that the incident is closed.

5. **Knowledge base**: All information generated during the treatment of the incident is used to inform and train colleagues and as reference material for future similar incidents.

Humanitarian organizations can base their SOPs on this 5-step model, describing how each step should take place within their organization. This should include the functions/roles and teams within an organization that are responsible at each stage of the process. These steps should be incorporated into or extended from existing incident response protocols (e.g. security incident management related to humanitarian access).

In a given response context, organizations should also work to integrate any joint incident management procedures into existing coordination structures, such as the clusters and mechanisms for inter- and intra-cluster coordination.

[7] The Centre for Humanitarian Data provides several sources of guidance that can inform the development of Data Incident Management SOPs on the **Data Responsibility page**.

[8] **How to handle incidents according to ISO 27001 A.16**, Antonio Jose Segovia, (October 2015.).

[9] For humanitarian organizations, an example of such a classification is the World Health Organization's (WHO) **International Classification of Patient Safety, Conceptual Framework for the International Classification of Patient Safety**.

[10] WHO, **Conceptual Framework for the International Classification of Patient Safety**.

RECOMMENDATIONS FOR IMPROVING DATA INCIDENT MANAGEMENT IN HUMANITARIAN ORGANIZATIONS

Introducing or improving data incident management in humanitarian operations is critical to more responsible data practice in the sector. The Centre for Humanitarian Data recommends that organizations focus on the following areas:

1. **Establish a common understanding of data incident management**
   Use a risk model to understand the causal chain that can lead to data incidents for specific offices and systems. Identify key threat actors and vulnerabilities for offices and systems and understand existing security controls and their effectiveness. Finally, map existing data incident management capacity and determine whether it is positioned appropriately. Once clear definitions and processes are articulated, invest in staff awareness and support a culture of open dialogue about incidents, in which proactive reporting and management of incidents is incentivized, not punished.

2. **Strengthen data incident management capacity**
   Take measures to put in place security controls to mitigate the risk of data incidents, and share best practice with partners. Build on existing work in the sector to fill governance gaps which can create vulnerabilities for your organization. Engage with organizational partners to set up information channels around data incidents. Share known vulnerabilities in a controlled manner with trusted counterparts for cross-organizational learning.

3. **Support continuous learning**
   Support learning and development of improved data incident management practices by organizing training and drills based on scenarios likely to occur in different operational settings. These exercises should occur regularly and may even involve multiple organizations training and drilling together. In addition, document actual data incidents as cases for internal knowledge development.

Organizations are encouraged to share their experience in the development of data incident management with the Centre for Humanitarian Data via centrehumdata@un.org.

COLLABORATORS: **YALE UNIVERSITY, JACKSON INSTITUTE OF GLOBAL AFFAIRS.**

The **Centre for Humanitarian Data** ('the Centre'), together with key partners, is publishing a series of eight guidance notes on Data Responsibility in Humanitarian Action over the course of 2019 and 2020. The Guidance Note series follows the publication of the **working draft OCHA Data Responsibility Guidelines** in March 2019. Through the series, the Centre aims to provide additional guidance on specific issues, processes and tools for data responsibility in practice. This series is made possible with the generous support of the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO).

This document covers humanitarian aid activities implemented with the financial assistance of the European Union. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Union, and the European Commission is not responsible for any use that may be made of the information it contains.

This project is co-funded
by the European Union