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 populations, organisations, and other individuals or groups.
- Examples of humanitarian data incidents include physical breaches of infrastructure, unauthorised disclosure of data, and the use of 'anonymised' beneficiary data for non-humanitarian purposes, among others.
- A data incident has four aspects: a threat source, a threat event, a vulnerability and an adverse impact.
- There are five steps to responding to data incidents: notification, classification, treatment, and closure of the incident, as well as 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 organisations overall might be well advised to listen to a quote from IT-security circles: 'There are two types of organisations: 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. Available here: **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf**

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 Organisation for Standardisation's (ISO) ISO Standard 27001 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 aspects: a threat source, a threat event, a vulnerability and an adverse impact. 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. Unauthorised 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 are presented to demonstrate how to think about identifying potential causal chains that can lead to data incidents and how these causal chains create context-specific forms of data incidents for humanitarian actors and affected populations.

[2] ISO 27001, available here: **https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en**

[3] NIST Computer Security Resource Center Glossary, available here: **https://csrc.nist.gov/glossary/term/threat**

[4] International Association of Privacy Professionals, *Is it an incident or a breach? How to tell and why it matters*, available here: **https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/**

RISK MODELS

The figure below presents a generic risk model with key risk factors that organisations can use to understand how threat events may occur. These threat events exploit existing vulnerabilities that are either magnified by predisposing conditions or mitigated by security controls already in place.

The exploitation of existing vulnerabilities by a threat event causes adverse impacts that produce organisational risk, which includes not only risks and potential impacts to the organisation but also to the individuals that the organisation seeks to serve.

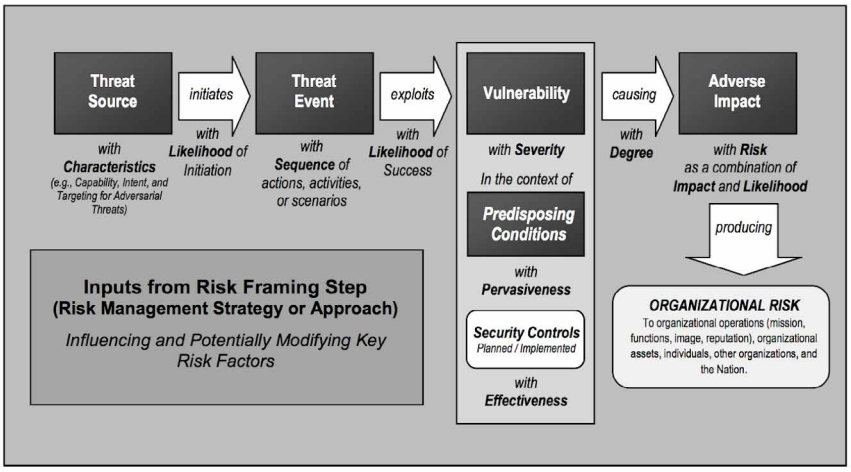

Figure 1. "Generic Risk Model with Key Risk Factors". Source: NIST Special Publication 800-30 pg. 12[5]

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

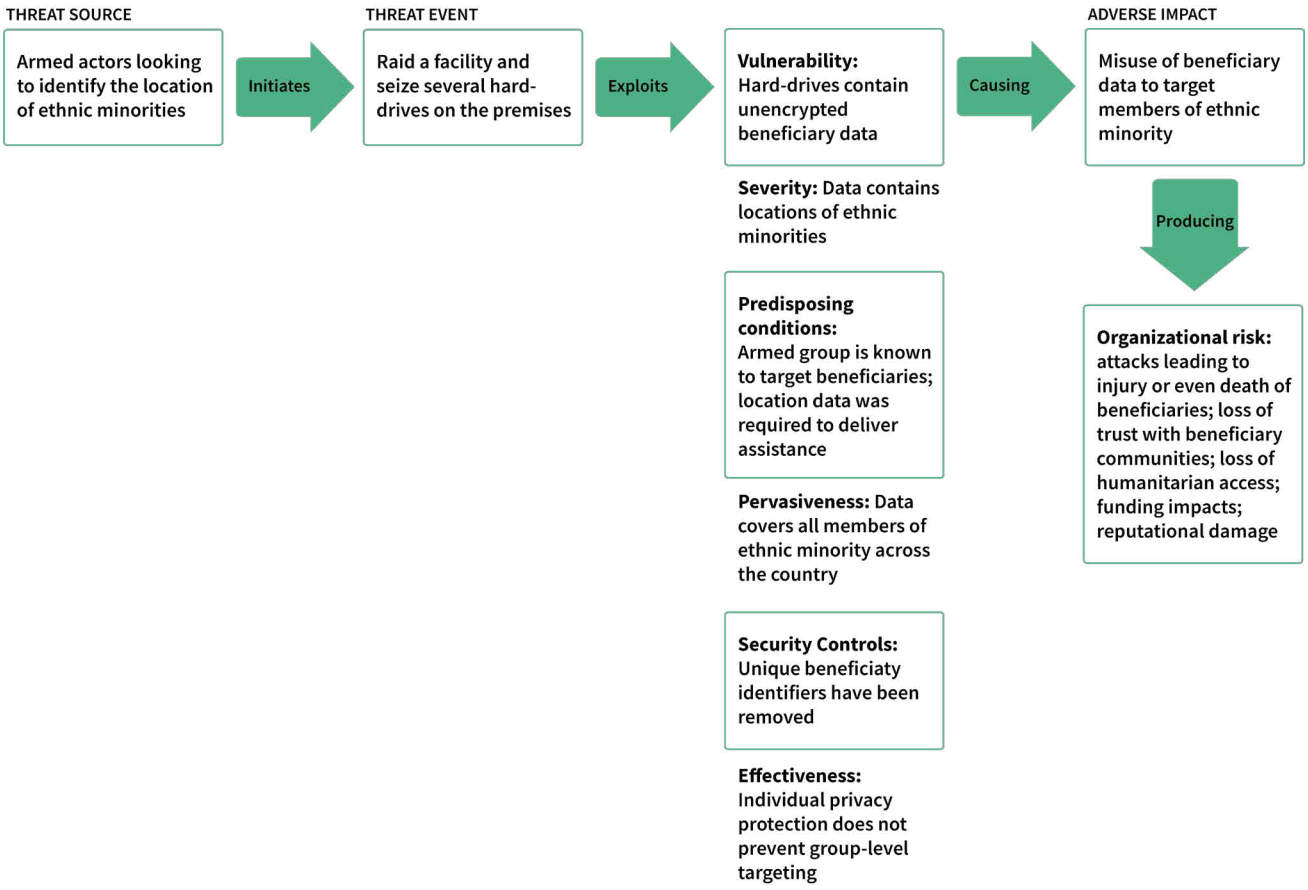

Figure 2. Risk Model with Key Risk Factors adapted to a humanitarian context.

[5] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments. Available here: **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf**

There are a number of complex components that organisations must think through in developing their own risks models related to data incidents. The nature of these components and how they come together to constitute a data incident will vary from one organisation to another and should be adapted to the specific operational realities within which different humanitarian actors deliver assistance.

STEPS IN DATA INCIDENT MANAGEMENT

After clearly defining what constitutes a data incident, organisations can begin developing the fundamental components of incident management. As the humanitarian sector lacks a clear approach to this work, it is helpful to look again to other sectors for guidance in this area.

The ISO suggests five components of industry best practice for security incident response. As shown in the image below, incident managers need to be able to 1) notify their organisations that an incident has occurred; 2) classify the nature of the incident; 3) treat the incident by rectifying the vulnerability and mitigating any potential harm; 4) formally close the incident; and 5) integrate learning from the event into the organisation's knowledge base.[6]

Figure 3: Five steps in the treatment of security incidents (Source: ISO 27001)[7]

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

- **Notification of the incident**: A person detects an event that may cause harm to the functioning of the organisation. The person communicates the incident according to the communication procedures of the organisation (usually an email, a phone call, a software tool, etc.).
- **Classification of the incident**: A person receives the incident notification and, depending on various parameters, it is classified. The person who detects the incident can also make a classification, but it is a technical expert who classifies it in the appropriate way.[8] It is essential that managing risk begins with classifying all types of potentially harmful incidents - whether or not tangible harm actually results from them.[9]
- **Treatment of the incident**: Once the incident is classified, and the severity and time agreed for its resolution are known, a technical expert needs to decide on the necessary measures to resolve it.
- **Closure of the incident**: Once the incident is solved, all the information generated during the treatment is recorded, and finally, the person who first sent notification of the incident is notified that it was closed.
- **Knowledge base**: All the information generated during the treatment of the incident is critical for possible similar incidents in the future, as well as to collect evidence.

[6,7] *Antonio Jose Segovia, How to handle incidents according to ISO 27001 A.16*, available here: **https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/**

[8] For humanitarian organisations, the World Health Organisation's (WHO) *International Classification of Patient Safety, Conceptual Framework for the International Classification of Patient Safety*, available here: **https://www.who.int/patientsafety/implementation/taxonomy/ICPS-report/en/**

[9] WHO, *Conceptual Framework for the International Classification of Patient Safety*, available here: **https://www.who.int/patientsafety/taxonomy/icps_full_report.pdf**

Building on this 5-step model, humanitarian organisations can create Standard Operating Procedures (SOPs) for how each step of the response chain should occur in the context of humanitarian operations. This should include the functions/roles and teams within an organisation 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, organisations 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.

AREAS FOR INVESTMENT: IMPROVING DATA INCIDENT MANAGEMENT IN HUMANITARIAN ORGANISATIONS

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 organisations and networks to invest in the following three areas:

A. Establish a common understanding
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.

B. Follow the steps for data incident management
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 organisation. Engage with organisational partners to set up information channels around data incidents. Share known vulnerabilities in a controlled manner with trusted counterparts for cross-organisational learning.

C. Support continuous learning
Support learning and development of improved data incident management practices by organising trainings and drills based on scenarios likely to occur in different operational settings. These exercises should occur regularly and may even involve multiple organisations training and drilling together. Document cases of data incidents for internal knowledge development.

Organisations 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**, together with key partners, will publish a series of 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 European Union Civil Protection and Humanitarian Aid Operations (DG ECHO). This guidance note was prepared in collaboration with Nathaniel Raymond, lecturer - Jackson Institute of Global Affairs, Yale University, and Yale students Gretchen Buermann, Chloe Jensen, and Olivia Mooney.