Data and Security Responsibilities of the Individual Humanitarian

June 2023

DH Network
Digital Humanitarian Network

Licensing Information

Data and Security Responsibilities of the Individual Humanitarian

By

Lidewij Heerkens (l.m.heerkens@student.tudelft.nl | LinkedIn)
Delft University of Technology

Andrej Verity (verity@un.org | LinkedIn)
United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA)

Design

Alexandra Sternin | alexsternin.com

This document was made possible with the support of

OCHA

Table of Contents

01 **Interviewees**

02 **Key Messages**

03 **Introduction**

05 **The Yawning Gap**

05 Problems with policies

06 Inconsistent practices

09 Burden of responsibility

11 **The Impossible Mission**

11 Complexity in the humanitarian sector

14 Undeniable Risk

15 **Needed Improvements**

15 Targeted education

17 Minimize the individual responsibility

17 Scenario and impact analysis of data

19 **Annex A: Methodology**

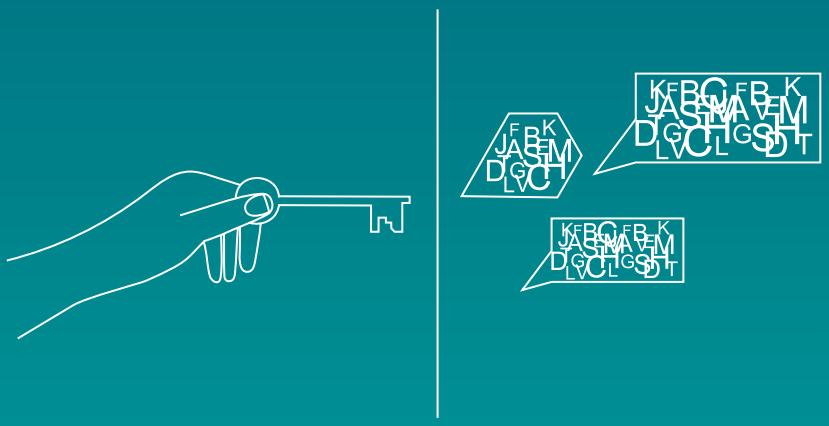
Interviewees

The authors would like to extend our deepest gratitude to the 15 individuals who took the time to meet with us to share details about their projects, lessons learned and recommendations. Without their contributions, this paper would not have been as compelling. This paper does not represent the views of the interviewees unless explicitly stated. This paper does not represent the views of the interviewees unless explicitly stated. The authors have drafted the paper based on a combination of literature review and interviews.

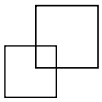
Name	Title	Organization
Alfonso Zabaleta	Access Officer	UNOCHA
-	Security Trainer at OICT	UN Secretariat
Daniel Gilman	Humanitarian Affairs Officer, Thailand	UNOCHA
Daniel Pfister	Humanitarian Affairs Officer	UNOCHA
Eero Sario	Senior Officer Primary Data Collection	IFRC
Emerson Tan	Information security expert	MapAction
Eva Vognild	Humanitarian Affairs Officer	UNOCHA
Lars Stevens	Operations Lead	510 Red Cross
-	Security Trainer at OICT	UN Secretariat
Miguel Angel Hernandez Rivera	Information Management Officer	UNOCHA
Olivia Williams	Principal Information Security and Strategic Analysis Consultant	Apache IX
Saeid Kdaimati	Information System Officer	UNOCHA
Tamas Foldesi	Senior Officer IT Security, IT Policies	IFRC
Thomas Braun	Chief Cybersecurity	UN Secretariat

Key messages

- Data security practices in the humanitarian sector cause increased risk since there are
  - > Disconnects between guidelines, policies, strategies and employees' data security practices.
  - > Inconsistencies in employees' data security practices in terms of sharing, storage and incident management.
  - > Dependencies on individuals to take their own security-related initiatives based on their personal knowledge of data security.
- Different perspectives of the state of data security in the humanitarian sector between HQ-based management and the realities faced by field operators.
- Unrealistic assumptions that the responsibility of data security can be (predominantly) put on the shoulders of individual humanitarian workers.
- Urgently needed improvements. Recommendations exist to improve the situation relatively quickly:
  - > Relieve the humanitarian worker's individual responsibility through automatization and less data collection.
  - > Improve training through new approaches, such as microlearnings.
  - > Institutionalize the Data Responsibility Officer role.
  - > Include scenario and impact thinking regarding data, as part of the standard requirements for all humanitarians.



Introduction



Humanitarian organizations provide aid to save lives, reduce human suffering and protect human dignity. To improve this aid, organizations' use and appliance of data are steadily increasing. However, this increase comes with challenges and opportunities.[1] Opportunities include faster communication, more accurate estimates and thus more accurate aid in crisis situations. For example, new sources of data, such as satellite data, enable activities from estimating the population of refugees in settlements[2] to tracking deforestation.[3] However, the increased use of data also leads to new challenges, of which data security is one of the largest.

Data security is defined as the practice of protecting digital information. A significant example of a data security breach was the cyberattack on the International Committee of the Red Cross (ICRC) in 2022. The breached data included personal information about vulnerable populations.[4] Such a breach can lead to real-world harm for those whom the sector aims to serve.[5]

Data leaks mostly involve individual mistakes by staff.[6] In the case of the ICRC cyberattack, individual practices also contributed to vulnerabilities in the system, namely the late application of critical patches.[7]

Organizations throughout the humanitarian sector have developed policies, strategies and guidelines to deal with data security challenges and prevent data incidents. However, The New Humanitarian points out that the data policies often lack actionability and practicality for humanitarian workers.[8] The translation of policies and guidelines to the actual application by individual humanitarian workers remains unclear. To identify possible improvements for the organization's data security, more insight is needed into the individual humanitarian worker's security practices.

1 Bell, D., Lycett, M., Marshan, A., Monaghan, A. (2021). Exploring future challenges for big data in the humanitarian domain. Retrieved from: www.sciencedirect.com/science/article/pii/S0148296320306172

2 Quinn, John. A, et al. (2018). Humanitarian applications of machine learning with remote-sensing data: review and case study in refugee settlement mapping. Retrieved from: royalsocietypublishing.org/doi/full/10.1098/rsta.2017.0363 United Nations (2022). Big data for Sustainable Development. Retrieved from: www.un.org/en/global-issues/big-data-for-sustainable-development

3 United Nations (2022). Big data for Sustainable Development. Retrieved from: www.un.org/en/global-issues/big-data-for-sustainable-development

4 ICRC (2022). Cyber attack on ICRC: What we know.

5 Irwin Loy (2022). Data Security in Frontline Aid. From The New Humanitarian.

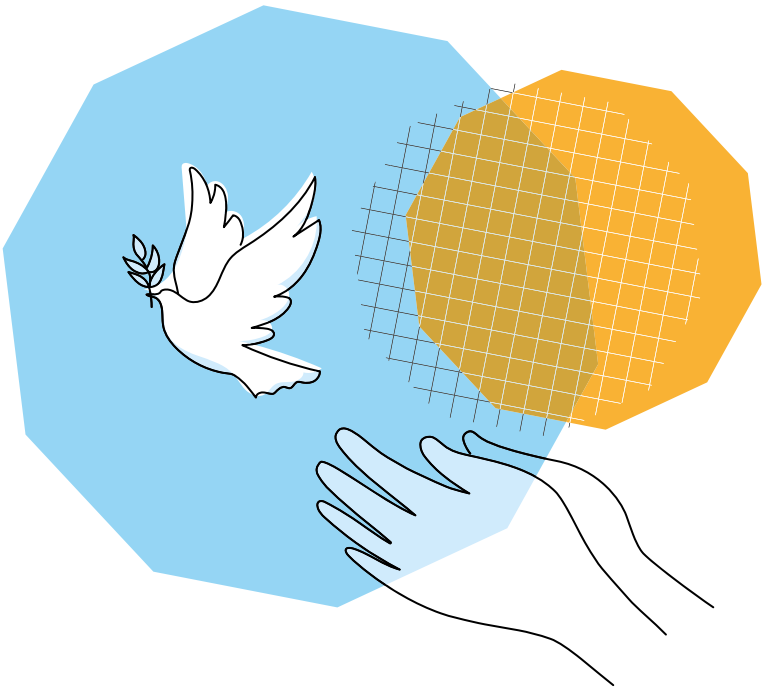
6 ScienceDirect (2022). Security Awareness Program. Retrieved from: www.sciencedirect.com/topics/computer-science/security-awareness-program

7 ICRC (2022). Cyber attack on ICRC: What we know.

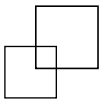
8 Irwin Loy (2022). Data Security in Frontline Aid. From The New Humanitarian.

To gain such insight in the humanitarian sector, the authors conducted several interviews to discuss and question humanitarian responders' personal data security behaviour. At the same time, an understanding of organizational approach and any room for improvement was evaluated by reviewing the current policies, strategies and data security guidelines in place (see annex A).

This paper outlines several specific recommendations for international humanitarian organizations like UNOCHA, their personnel and the sector at large. The paper aims to speak to anyone in an international humanitarian organization looking to improve individual data security practices.



The Yawning Gap



The humanitarian sector has made recent and committed efforts to improve data practices. In 2020, ICRC published a data protection handbook.[9] The following year, the Inter-Agency Standing Committee (IASC) published its Operational Guidance on Data Responsibility in Humanitarian Action,[10] UNOCHA finalized its data responsibility guidelines[11] and IFRC introduced a Data Playbook with practical exercises.[12] Efforts by IASC and UNOCHA are intended to encourage others to take data responsibility seriously, which means ensuring humanitarian data is used safely, ethically and effectively. The IFRC playbook and the ICRC handbook focus more on the individual data security practices intended to tackle the day-to-day practices and procedures established in humanitarian action. However, these efforts have not been consistently implemented. **A gap remains between the intended and the actual practices.**

Problems with policies

The first elements that contribute to this gap are the policies and guidelines themselves. The guidelines previously mentioned are not mandatory for humanitarian workers. The UN's current mandatory policies are gravely outdated, and the policies provided for individual employees are from 2004 and 2007. The 2007 policy still recommends to print a hard copy of classified information received in electronic form.[13] But for many years, printing sensitive documents has been neither realistic nor the preferred method to ensure security.

The volume of guidelines and tip sheets is, mildly put, extensive, and documents are often lengthy. For example, the ICRC handbook contains 312 pages. As one can imagine, this does not inspire or invite employees to educate themselves on data security practices.

9 International Committee of the Red Cross (2020). Handbook on Data Protection in Humanitarian Action.
10 Inter-Agency Standing Committee (2021). Operational Guidance on Data Responsibility in Humanitarian Action.
11 Centre for Humanitarian Data (2021). OCHA Data Responsibility Guidelines.
12 PrepareCenter (2022). The Data Playbook by IFRC.
13 United Nations Digital Library (2007). Information sensitivity, classification and handling.

Inconsistent practices

Consistency is key when it comes to data security. If one employee applies best practices and another does not, everyone's security efforts become less effective, as the organization can still be compromised.[14] The authors found that the compliance of data security practices with protocols and guidelines differs significantly between office and employee. This discrepancy is due to security practices coming from one's own knowledge and initiative combined with poor communication and training.

> *"In 2021 I was checking the UN Intranet and I found an article where the Secretary-General expressed the request to not use WhatsApp for any kind of communication, and I was really surprised because here [in the field] WhatsApp is the easy way to communicate."*[15]

Employees' data-related practices can differ wildly. In the case of WhatsApp, the practice is not in line with existing guidelines and protocols. The differences are clearly illustrated when it comes to data sharing. In the UN Secretariat, email and SharePoint are generally used for sharing on a regular basis. But when the information is sensitive, employees often prefer to share information offline, person-to-person.[16] For example, one employee asks the IT team to set up a secure location to exchange information,[17] whereas another employee uses applications such as Signal.[18] Variations exist based on local needs, especially when collaborating with the wider sector and/or the local population. With such individual-driven practices, challenges mount for an organization to ensure overall security. Lists of approved services exist, but employees also use non-approved services, as illustrated with the case of WhatsApp. How can an organization ensure security across what may feel like an endless number of services?

The inconsistencies at the UN partly stem from the current training programme. Many employees complete only a two-hour mandatory training programme on data security at the beginning of their career. Feedback, rewards and incentives are absent in the training. Imagine an employee who has worked at the UN for 20 years and has never, or rarely, been updated on data security. Things change quickly in the technology world; continual or frequent learning is necessary.

14 Interview with Emerson Tan, 26 October 2022.
15 Anonymous interviewee, 2022.
16 Interview with Miguel Angel Hernandez Rivera, 14 September 2022.
17 Interview with Daniel Pfister, 21 September 2022.
18 Interview with Alfonso Zabaleta, 20 September 2022.

> *There is a bit of a gap in training. We've designed our trainings to focus on things like phishing scams, while we should have more of a case study approach. A big part is being cautious about what kind of data we're collecting and storing."*[19]

On a voluntary basis, UN employees can join a cybersecurity awareness discussion platform within the organization or attend online sessions during the UN's annual Cybersecurity Awareness Month. The cybersecurity platform shows a high participation of employees with a technical background, such as information system officers, thereby demonstrating that the voluntary approach means most participants are already knowledgeable. Employees who are unaware of their own poor practices or uninterested in the topic are not sufficiently targeted and encouraged to participate.

Knowledgeable employees take action based on their own initiative to improve data security practices. Such employees reach out to their supervisors or the IT department to discuss and tackle data security challenges. If they encounter roadblocks to getting their work done, many resort to tools or services identified through their own initiative and occasionally pay for them out of their own pocket. Organizations do not offer to pay for password managers or additional virtual private network (VPN) services, yet both are considered useful.[20] The result is that data security is highly dependent on the individual rather than the organization's policies and guidelines.

> *When I have those projects [projects that make the interviewee reflect on data security practices], it's really sensitive personal data. I want to make sure that I do the right thing, so I discussed with IT and data-responsibility colleagues a lot. We decided to store the data in a password-protected Excel file within an encrypted ZIP file on a dedicated place on the corporate SharePoint site with restricted access. After the project was completed the data was then destroyed."*[21]

19 Anonymous interviewee, 2022.

20 Interview with Eero Sario, 14 October 2022.

21 Interview with Daniel Pfister, 21 September 2022.

IT services provided by organizations are subject to change and can lead to messy transitions.[22] This can lead to an erosion of trust in the organization's ability to offer appropriate solutions.

> *We moved the section's content from Google Drive to SharePoint but have not kept it very organized, it would require some cleaning. I still also keep some back-ups on external hard drives, such as USB."*[23]

Another challenge is the inadequate services provided, thus impacting the efficiency of regular work activities. Such inadequacy leads to shadow IT[24] (using services prohibited by the organization). As employees and teams within organizations select and manage their own services, the organization's control over the security is negatively impacted.

> *There is no convenient way to work on MS Office files with people outside our organization. It's a constant issue, especially in operations. If the IT policies prevent collaboration, people will find ways to circumvent them to get the work done."*[25]

22 Interview with Eva Vognild, 20 September 2022.
23 Ibid.
24 Interview with Eero Sario, 14 October 2022.
25 Ibid.

Burden of responsibility

The responsibility of ensuring data security is distributed throughout the entire organization, and among all teams and individuals, from senior management to the lowest level. All practices need to be up to a certain standard to ensure security, from employee practices to the technical infrastructure. Data breaches happen through the path of least resistance.[26]

> *"You can't disentangle the organization from the individual. Because a lot of what is required has to be done at an organizational level. If you can't afford the infrastructure to actually keep data safe at an organizational level, then everything you do at an individual level is kind of pointless."*[27]

The current responsibility put on the individual employee is a heavy burden, especially with the limited training and support to implement protocols. In the humanitarian sector, the focus tends to be on awareness and active participation,[28] leading to humanitarian employees having to take their own initiative to learn and implement responsible behaviour. This approach passes the burden from HQ and management to field officers.

> *"We do rely on some active participation. From within the offices to identify the needs, but also then to help or actually facilitate the transmission and then the training themselves."*[29]

26 Interview with Emerson Tan, 26 October 2022.
27 Ibid.
28 Interview with Thomas Braun, 21 October 2022.
29 Anonymous interviewee, 2022.

When officers have questions and are proactive in figuring out how to improve data security practices, the support is not always available, or employees do not always know where to look for it. Even though there is sufficient knowledge surrounding data security in the organization, the knowledge is not used enough to support all employees. On top of that, employees do not always know where to go with questions.

> *"For me, I would like to know where to go with questions. For example, I have questions considering VPN. What VPN is recommended, and what are the pluses and minuses of different layers of encryption? We do have very good IT support, but she is not a data security specialist. From within the offices to identify the needs, but also then to help or actually facilitate the transmission and then the training themselves."*[30]

In practice, and even with good intentions, the own-initiative approach often contributes to inconsistencies in data security practices. On the one hand, it could be said that employees neglect responsibility. On the other hand, when it is a recurring problem, one could argue that the organization's expectations on compliance with policies and guidelines are unrealistic and that a different strategy may be required. This is especially true given that the existing policies are not translatable to the field.

> *"Organizations often put the responsibility of aligning with policy squarely on the shoulders of the aid worker, but in actual fact, data security policies rarely fit the context in which aid workers find themselves, and organizations can't expect people to adhere to policy when that's the case."*[31]

30 Ibid.

31 Interview with Olivia Williams, 18 November 2022..

The Impossible Mission

Weaknesses have been pointed out. But now what? The issues are complex and difficult to tackle. Data security is a wicked challenge, meaning there is no single solution to completely ensure data security throughout the whole organization. Data security can only be made better or worse.[32] Consistent effort and prioritization at every level of the organization are essential for improvement. No singular, watertight approach exists to data security, but there is still a serious need to increase resistance through multiple, overlapping solutions at different levels of the organization, thus lowering the chance of a breach.

> *"That [data security] is mission impossible. Each time I leave a conference or any sort of cybersecurity event, I always leave with the impression that's never going to end and there is no silver bullet. No one knows what the solution is."*[33]

Complexity in the humanitarian sector

Data security is a complex issue made even more so due to the sector's operating environment.

First, humanitarian organizations tend to be large and have diverse staff.[34] The size of the workforce makes it challenging to target the whole workforce. The diversity leads to different levels of data literacy and knowledge. The challenge remains to create consistency and achieve a certain standard for data security.

Second, humanitarian organizations rely on donor funding, which brings two challenges. The first is that allocating funding to data security can be difficult because the funds are competing with many humanitarian programmes – sometimes life-saving ones. If organizations do not invest in security, employees can be left to feel that they need to invest in security practices themselves, thereby leaving the larger organization vulnerable.

32 Kevin Gilmore (2018). Cyber Security: A Wicked Problem. Retrieved from: www.dafitc.com/cyber-security-a-wicked-problem/

33 Interview with Tamas Foldesi, 17 October 2022.

34 Interview with Thomas Braun, 21 October 2022.

> *We have entities that either have particularly sensitive data or development teams that develop applications who obviously need to be able to manage credentials in a more secure way. We encourage the use of those additional tools in general, and we specifically encourage it in what we call high-risk-use cases. However, unless the organization is able to provide the tooling and the funding to use those tools, we cannot really mandate it.*"[35]

The second challenge with relying on donor funding is that the funding itself often is not influenced by the actual impact of the programmes or the project's needs (like data security).[36] When major data incidents happen, unfortunately it is rare to see funding increase for data security.[37] At the management level, one of the largest dilemmas is the availability of funds to invest in data security.[38] Are donors willing to invest in a humanitarian organization's data security and all that it entails (data management, personnel training, back-end solutions, long-term maintenance, etc)? Or do they prefer to fund life-saving activities (e.g. a field hospital)? Is management willing to divert some programme funding to data security? How can security improvement be measured and reported back to donors?

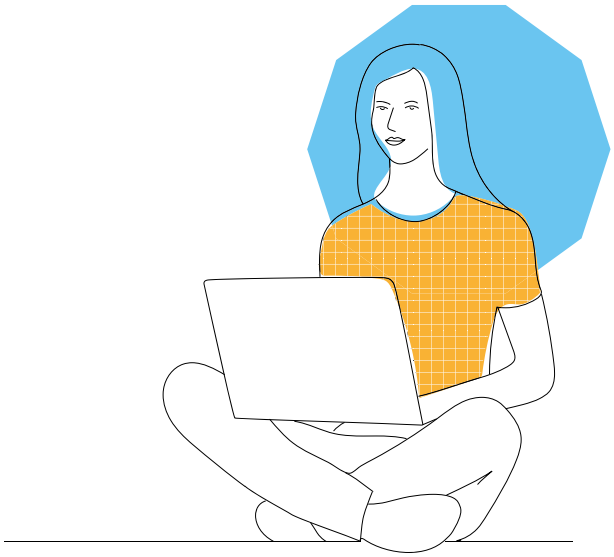
> *Here is a really key problem, right. Negative impacts on the beneficiaries do not figure at all into funding decisions. For example, if beneficiaries end up dying, that has zero effect on my ability to raise funds. There's no detrimental consequences when beneficiaries end up negatively impacted as a result of my actions.*"[39]

Third, humanitarian organizations tend to be slow and rigid. Globally, technological development

35 Anonymous interviewee, 2022.
36 Interview with Emerson Tan, 26 October 2022.
37 Ibid.
38 Interview with Thomas Braun, 21 October 2022.
39 Interview with Emerson Tan, 26 October 2022.

is happening at a rapid pace,[40] but humanitarian organizations struggle to keep up with the change. Regular change in policies and training is needed to maintain suitable data security practices for the new technologies. A data security policy originating from a time when the iPhone did not even exist[41] is definitely not sufficient to ensure data security in today's era.

> *"When I joined, our organization had only two mandatory trainings. Although an audit clearly recommended that cybersecurity training must be mandatory, it took three years to make that happen, since the organization wanted to limit the number of mandatory trainings."*[42]



40 Francesca Giovannini and Kathryn Moffat (2017). Technology in a Time of War: Humanitarian Aid at an Inflection Point. From the American Academy of Arts and Sciences.

41 Wikipedia (2022). iPhone (1st_generation)

42 Anonymous interviewee, 2022.

Undeniable Risk

The current state of data security in the humanitarian sector contains many unarticulated risks.[43] The problem with unarticulated risk is that the risks do not weigh into the decision-making. Working with data comes with certain risks, such as it falling into the wrong hands. Within the humanitarian sector, decisions are often made without considering the potential impact of losing control over information.[44]

> *"Risk acceptance must be explicit in a way that the organization's chief stakeholder explicitly accepts the risk of something going wrong with the decision. I'm not advocating for humanitarian organizations never balancing safety. That doesn't always work because we have the time element. We need to react quickly, and sometimes quick means you have less time for other things like extensive security, for example, which could be fine. However, we may take them [risks] without articulating them, without making them visible, without formally approving them."*[45]

Inclusion of risk assessment is necessary. However, risk is challenging to define and measure. There are various methods of measuring risk, ranging from operational impact to financial costs. Understanding and preparing for risk is a major topic, and this paper does not have room to do it full justice. Readers should explore risk management; a good starting point would be the OCHA Data Responsibility Guidelines, and developing a data impact assessment template for humanitarians, with a focus on risk.[46]

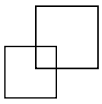
43 Ibid.

44 Interview with Tamas Foldesi, 17 October 2022.

45 Ibid.

46 Centre for Humanitarian Data (2021). OCHA Data Responsibility Guidelines.

Needed Improvements



We need a cultural shift in the humanitarian sector,[47] but this certainly will not happen overnight. Ensuring data security is a complex challenge with many dilemmas, and credit needs to be given to previous and ongoing work. Some of the recommendations have been mentioned in guidelines such as the IASC's Operational Guidance on Data Responsibility In Humanitarian Action.[48] The UN Secretariat is making efforts to tackle some of the above-mentioned issues within budgetary constraints,[49] including by creating recurrent trainings.[50]

To provide recommendations that are as practical and achievable as possible, limitations and dilemmas are kept in mind. These recommendations aim to provide a short but complete and comprehensive overview of the most urgent and quick improvements needed for the humanitarian sector from the interviewees' perspectives.

Targeted education

Currently, the mandatory data security education in organizations is limited. For example, in the case of UNOCHA, only a two-hour online course is mandatory. This is a "one and done" arrangement, whereby employees do not need to refresh their knowledge. A new approach to training data security is needed.[51] First, training needs to be recurring and more user friendly. One solution is microlearnings, which are short, online (+/- 2 minutes) learnings repeated over time. At IFRC, such learnings showed very high engagement (~80%). [52,53] This approach could be used to ensure a certain minimal standard.

Second, the trainings need to be paired with a regularly updated organization-level website that includes simple and basic practices.[54] Compiling and maintaining such resources[55] on a webpage would be a considerably easy and cheap improvement. Connecting it to the trainings would make it ever more prominent and impactful. Unfortunately, at this time, one can point to examples such as the UN's mandatory

47 Interview with Olivia Williams, 18 November 2022; interview with Lars Stevens, 31 October 2022.

48 Inter-Agency Standing Committee (2021). Operational Guidance on Data Responsibility in Humanitarian Action.

49 Interview with Security Trainer at OICT, 7 November 2022.

50 Ibid.

51 Interview with Saeid Kdaimati, 28 October 2022.

52 Interview with Tamas Foldesi, 17 October 2022.

53 80 per cent comprises 60 per cent fully completed and 20 per cent partially completed.

54 Interview with Lars Stevens, 31 October 2022.

55 Data Responsibility Team, Centre for Humanitarian Data (2022). Guidance Note On Data Security In Operational Data Management.

training still linking to the outdated policies of 2004 and 2007. Such glaring omissions cannot be allowed to continue if we are to take security seriously.

Standard training needs to be supplemented with more personalized training to meet the different needs throughout an organization. Different locations and work processes require tailored, context-specific training that needs to adjust to the data literacy per individual.[56] In-person trainings are preferred because online participants tend to disconnect at some point.[57]

Furthermore, the interviews showed that employees don't always know where to go with data security questions.[58] A **visible and knowledgeable Support Officer** is necessary to support training-and-knowledge needs and to complement the organization's skill level. The Support Officer should be implemented per organization or per department, depending on the number of employees. He or she can help answer questions and have yearly sessions with offices or small groups of employees to reflect and discuss data security practices.

Put together, the microlearnings, the website and the Support Officer would tackle the issue of the perceived limited available support.

Lastly, **reward and exhibit good data security behaviour**. By rewarding projects that have been done well, more good behaviour and funding will follow.[59] Depending on the reward, it could be seen as a serious incentive for some employees.[60] Incentives could be monetary, emotional or a service.[61] Rewards could be implemented per office or team and given by supervisors or managers. With flexibility, the rewards could be identified by asking employees what would incentivize them to improve their data security practices.

56 Interview with Olivia Williams, 18 November 2022.

57 Interview with Security Trainers at OICT, 7 November 2022.

58 Interview with Daniel Gilman, 14 November 2022.

59 Interview with Lars Stevens, 31 October 2022.

60 ScienceDirect (2022). Security Awareness Program. Retrieved from: www.sciencedirect.com/topics/computer-science/security-awareness-program

61 Interview with Olivia Williams, 18 November 2022.

Minimize the individual responsibility

The expected data security practices for individual employees are challenging for a significant portion of employees. Shrinking the responsibility while improving data security practices can happen through the following actions:

Proper use of software. The IT department can support data security through software implementation. First, increase the use of **role-based access**, which limits unnecessary access to data.[62]

Second, leverage as much **automation** as possible.[63] Examples include enforcing multifactor authentication (MFA), automatically executing security updates and forcing users to select a sensitivity level before sending a file by email.

Third, expand the list of **standard software**[64] that employees are allowed to use.[65] If software is being used that is not standard, there is an unfilled need. Instead of prohibiting its use, standardize the (new) software and make agreements with relevant providers to ensure security, thereby preventing shadow IT.

Do not collect data that cannot be protected.[66] For example, if one is working in the field and the collected data is being shared with a questionable Government, then sensitive information (e.g. ethnicity) should not be gathered. The same principle applies for storage: If you do not need to store the data, delete it. When it comes to reducing the impact of a hack, if the data has low 'value' to a hacker, then the impact will be reduced and less likely to be worth the hacker's effort. [67]

Scenario and impact analysis of data

To make a well-informed decision on what data security practices should be in place, conducting a scenario analysis of data is essential. The scenario analysis challenges employees to think about the potential impact in multiple scenarios. The analysis should become part of employees' habits. At this time, security decisions are often made without considering the scenario of losing control over the data.[68] Conducting a scenario analysis helps to identify preventive measures and can even lead to not collecting data at all.

Humanitarians are not used to thinking from the bad person's perspective,[69] but this way of thinking is

62 Interview with Lars Stevens, 31 October 2022.

63 Interview with Saeid Kdaimati, 28 October 2022.

64 UN ICT Standards for Hardware and Software: iseek-external.un.org/system/files/current_standards.pdf, accessed February 2023.

65 Interview with Saeid Kdaimati, 28 October 2022.

66 Interview with Emerson Tan, 26 October 2022.

67 Ibid.

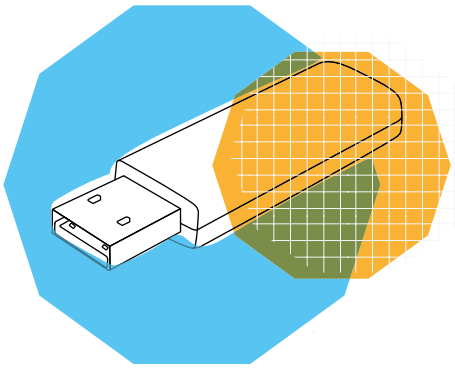
68 Interview with Tamas Foldesi, 17 October 2022.

69 Interview with Emerson Tan, 26 October 2022.

urgent and necessary. Lessons could be learned on how non-UN organizations consider the bad guy's perspective and the resulting scenarios.[70] Getting people to work through the IASC template for a data impact assessment would be a great start for many teams and offices.[71] These examples show how we circle back to the other recommendations of targeted education and minimizing responsibility. Mandatory training should include a data impact assessment, and software could provide users with proactive prompts.

> *"Imagine you plug in a USB and a pop-up shows up stating: 'We noticed you inserted a USB. Remember there was a data leak recently through aid workers using a USB."*[72]

Any one of these needed improvements may be achievable on their own, but only a concerted effort to address them all throughout the organization will result in an efficient, highly functioning, data-secure organization. To do this, there will need to be a shift in organization policies, a restructuring of fund allocations, dedication to continual learning/training and prioritization of staffing. Traditionally, organizations may have written off such efforts as too costly. But in today's era we now have little choice. Without action, organizations only increase the risk of being hacked or inadvertently exposing sensitive data, thereby harming the reputation of the organization and of those whose data was stored. Therefore, prioritizing data security practices is critical to ensure that the humanitarian sector can continue to focus on doing good.

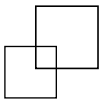


70 Interview with Olivia Williams 18 November 2022.

71 Inter-Agency Standing Committee (2021). Operational Guidance on Data Responsibility in Humanitarian Action.

72 Interview with Olivia Williams, 18 November 2022

Annex A: Methodology



The study's goal is to retrieve insight in data security practices, perspectives and opportunities. An exploratory study on data security in the humanitarian sector was carried out by exploring humanitarian websites and articles on data security in the humanitarian sector, and by talking to UNOCHA employees. Policies and guidelines were then reviewed to understand expectations for data security practices and responsibilities considering data security.

The following documents were included:

- The IASC Operational Guidance on Data Responsibility in Humanitarian Action (2021)
- The Centre for Humanitarian Data's Data Responsibility Guidelines (2021)
- The ICRC Handbook on Data Protection in Humanitarian Action (2020).
- The IFRC Data Playbook from PrepareCenter.org (2022).
- Guidance Note On Data Security In Operational Data Management of the Centre for Humanitarian Data's Data Responsibility Team (2022).
- Information sensitivity, classification and handling of United Nations Digital Library (2007).
- Use of information and communication technology resources and data of United Nations Digital Library (2007).

The topics in the guidelines and policies were revisited in the interviews. The paper is predominantly based on the interviews. Interviews were the preferred method of data collection, since understanding how data is handled throughout the organization can be sensitive and is often generalized in public reports. The emphasis is thus on perspectives and perceived opportunities. In the first instance, a diverse group of interviewees from different regions, organizations and positions was approached to include different perspectives. However, the interviewees do not represent the full range of humanitarians' perspectives. Bias could exist based on the contact list and whether the interviewees were willing or able to discuss data security.


DH Network
Digital Humanitarian Network