OCHA centre for humdata

THE CENTRE FOR HUMANITARIAN DATA

SÉRIE DE NOTES D'ORIENTATION
LA RESPONSABILITÉ DES DONNÉES DANS L'ACTION HUMANITAIRE

NOTE #2: LA GESTION DES INCIDENTS LIÉS AUX DONNÉES

POINTS CLÉS :

- Les incidents liés aux données humanitaires sont des événements impliquant la gestion des données qui ont causé des préjudices ou sont susceptibles de causer des préjudices aux populations touchées par les crises, aux organisations et à leurs opérations, ainsi qu'à d'autres personnes ou groupes.
- Parmi les exemples d'incidents liés aux données humanitaires, mentionnons les atteintes physiques à l'infrastructure, la divulgation non autorisée de données et l'utilisation des données des bénéficiaires à des fins non humanitaires, entre autres.
- Un incident lié aux données comporte quatre aspects : une source de menace, un évènement de menace, une vulnérabilité et un impact néfaste.
- Il y a cinq étapes pour réagir aux incidents liés aux données : la notification, la classification, le traitement et la clôture de l'incident, ainsi que l'apprentissage.

QU'EST-CE QU'UN INCIDENT LIÉ AUX DONNÉES DANS L'ACTION HUMANITAIRE ?

Dans le secteur humanitaire, les incidents liés aux données sont des événements impliquant la gestion des données qui ont causé des préjudices ou sont susceptibles de causer des préjudices aux populations touchées par les crises, aux organisations humanitaires et à leurs opérations, ainsi qu'à d'autres personnes ou groupes. Ces événements peuvent exploiter ou exacerber les vulnérabilités existantes.[1] Dans certains cas, ils peuvent également créer de nouvelles vulnérabilités susceptibles d'augmenter le risque de futurs incidents liés aux données.

Les travailleurs humanitaires n'ont ni une compréhension commune de ce que représente un incident lié aux données, ni défini un standard technique minimum quant à la manière dont ces incidents doivent être évités et gérés. La manière dont le secteur humanitaire développe des outils et met en œuvre des procédures de gestion des incidents liés aux données jouera un rôle important dans l'évolution des standards éthiques, techniques et professionnels des opérations humanitaires, ainsi que des droits humains.

> « Si les acteurs humanitaires numérisent davantage leurs données et leurs communications, ils ont un besoin urgent d'accroître leurs efforts en sécurité numérique. Bien que certains acteurs développent des outils de protection prometteurs, les organisations humanitaires dans l'ensemble auraient sans doute intérêt à prendre note de la citation suivante provenant des cercles sur la sécurité informatique : « Il existe deux types d'organisations : celles qui ont été piratées et celles qui le seront. »
>
> - Rahel Dette, Do No Digital Harm: Mitigating Technology Risk in Humanitarian Contexts

[1] « On entend par vulnérabilité une faiblesse dans un système d'information, des procédures de sécurité du système, des contrôles internes ou une mise en œuvre susceptible d'être exploitée par une source de menace. » **NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk**

Parmi les incidents liés aux données humanitaires, mentionnons les atteintes physiques à l'infrastructure, la divulgation non autorisée de données et l'utilisation des données des bénéficiaires à des fins non humanitaires, entre autres. Les incidents liés aux données peuvent également se produire sans que l'infrastructure technique ne soit compromise de quelque manière que ce soit. La collecte, l'utilisation et le partage légitimes de données par des humanitaires peuvent encore avoir des implications opérationnelles susceptibles de constituer un incident dans les cas où des rumeurs, des sensibilités culturelles, des dynamiques politiques et d'autres facteurs entraînent des effets préjudiciables liés aux données.

CADRES ET DÉFINITIONS POUR COMPRENDRE LES INCIDENTS LIÉS AUX DONNÉES

Les gouvernements et le secteur privé ont élaboré des cadres et définitions pour mieux comprendre les incidents liés aux données et qui servent de références utiles au secteur humanitaire.

- La norme ISO 27000 de l'Organisation internationale de normalisation (ISO) définit un « incident critique » comme « un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information ».[2]

- Le NIST (United States Department of Commerce National Institute for Standards and Technology) définit un événement indésirable impliquant une « cyber menace » comme « un événement ou une condition susceptible de provoquer une perte d'actifs et les conséquences ou l'impact indésirables de cette perte ».[3]

- Mahmood Sher-Jan de l'International Association of Privacy Professionals (IAPP) identifie trois autres catégories d'événements qui élargissent la définition des événements indésirables du NIST. Il s'agit, par ordre de gravité croissant, d'incidents de sécurité, d'incidents liés à la confidentialité et de violations des données.[4]

Exemples d'incidents possibles liés aux données humanitaires

Un incident comporte quatre facteurs : une source de menace, un évènement de menace, une vulnérabilité et un impact néfaste.[5] Vous trouverez ci-dessous deux types d'incidents hypothétiques susceptibles de se produire dans des contextes humanitaires.

Le premier scénario est un incident type de violation des données placé dans le contexte d'un conflit armé. Le second est un exemple du type de vulnérabilités qui peuvent déclencher des incidents liés aux données propres au secteur humanitaire.

1. L'accès non autorisé aux données se produit **[impact]** en raison de la présence d'acteurs armés **[source]** lors du pillage d'une installation et de la saisie de disques durs contenant des données bénéficiaires **[événement]**. Les disques durs n'étaient pas cryptés **[vulnérabilité]**.

2. L'absence de directives limitant la collecte de données à un but spécifique **[vulnérabilité]** aboutit à ce que le personnel recueille des données sur le statut matrimonial des femmes enceintes **[source]**. Une violation des données **[événement]** se produit par la suite, entraînant une augmentation des risques de violence physique **[impact]** contre les bénéficiaires enceintes non mariées.

Ces scénarios permettent de comprendre la démarche nécessaire à l'identification de chaînes de causalité susceptibles de créer des incidents liés aux données spécifiques à un contexte.

[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.

MODÈLES DE RISQUE

Le schéma ci-dessous présente un modèle de risque générique avec des facteurs de risque dont les organisations peuvent se servir afin de comprendre comment un incident lié aux données peut se produire. Un événement de menace exploite une vulnérabilité existante qui est soit amplifiée par des conditions préexistantes, soit atténuée par des contrôles de sécurité déjà en place. Cela entraîne des impacts négatifs qui engendrent des risques organisationnels, qui peuvent inclure des risques pour l'organisation et pour les personnes affectées.

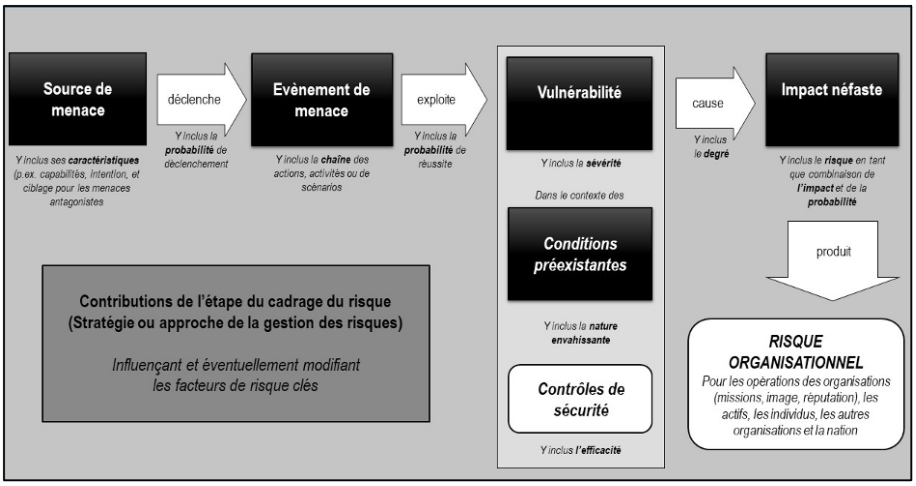

Figure 1. « Modèle générique de risque avec facteurs de risque clés ». Source : NIST Special Publication 800-30 pg. 12

Le schéma ci-dessous présente un exemple de la façon dont ce modèle générique de risque pourrait être adapté au secteur humanitaire.

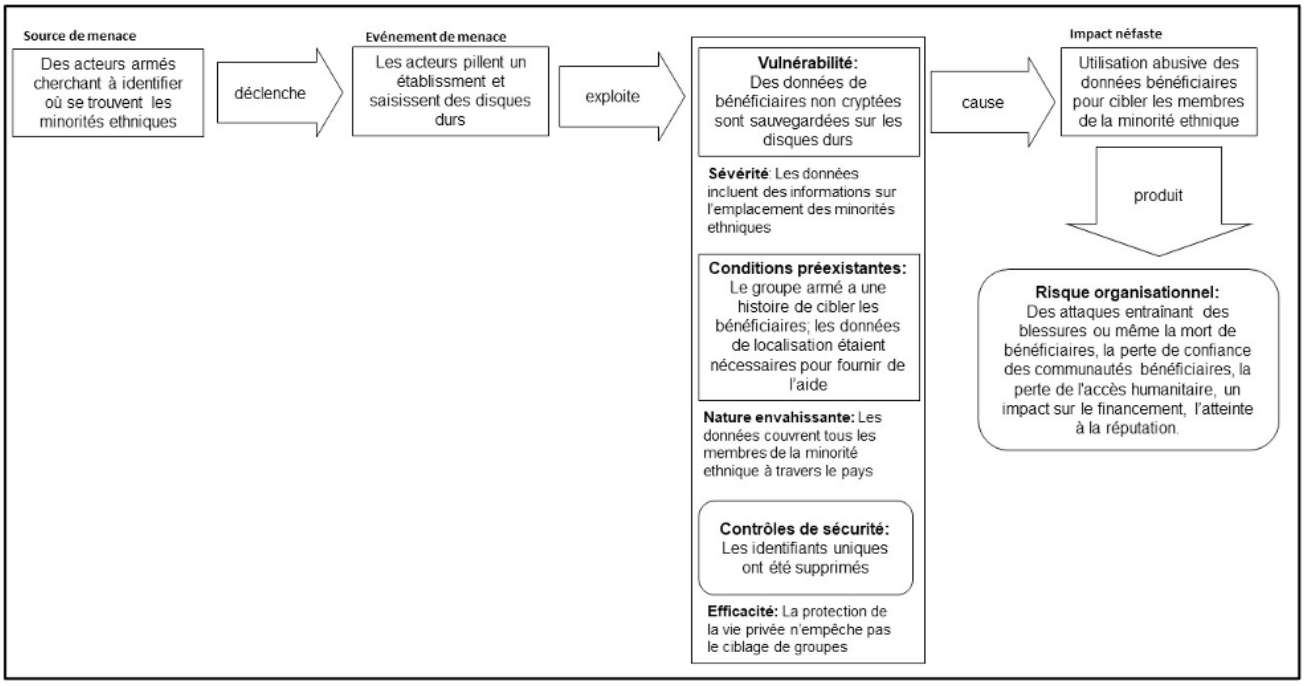

Figure 2. Risk Model with Key Risk Factors adapted to a humanitarian context.

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

Les organisations humanitaires peuvent développer leurs propres modèles de risque spécifiques pour la gestion des incidents liés aux données en tenant compte de ces facteurs. La nature de ces facteurs de risque et la façon dont ils se réunissent pour constituer un incident lié aux données varient d'une organisation à l'autre et doivent être adaptés à des réalités opérationnelles spécifiques.

ÉTAPES DE LA GESTION DES INCIDENTS LIÉS AUX DONNÉES

Après avoir clairement défini ce qui constitue un incident lié aux données, les organisations peuvent développer des procédures opérationnelles standard (POS) pour la gestion de tels incidents.

Les POS de gestion des incidents liés aux données doivent comprendre les 5 étapes suivantes : 1) .[7]

Figure 3: Cinq étapes pour le traitement des incidents de sécurité
(Source : How to handle incidents according to ISO 27001 A.16, Antonio Jose Segovia)[8]

L'application de ces étapes dans une organisation peut se présenter comme suit :

1. **Notification de l'incident** : Une personne détecte un incident et informe ses collègues responsables en fonction des procédures de communication définies de l'organisation (généralement un e-mail, un appel téléphonique, un outil logiciel, etc). Une notification doit contenir, si possible, une description des principaux facteurs de risque impliqués dans l'incident : source, événement, vulnérabilité et impact.

2. **Classification de l'incident :** Le destinataire de la notification classe l'incident en fonction de son impact (élevé, moyen ou faible) et de l'urgence du traitement (élevé, moyen ou faible).[9] La gestion des risques commence par la classification de tous les incidents, que des préjudices tangibles en résultent ou non.[10]

3. **Traitement de l'incident :** Un expert technique décide des mesures nécessaires pour traiter l'incident une fois que l'incident a été classé et que le délai de traitement a été convenu.

4. **Clôture de l'incident :** Toutes les informations générées pendant le traitement sont enregistrées et la personne qui a envoyé la première notification de l'incident est informée que l'incident est clos.

5. **Base de connaissances :** Toutes les informations générées lors du traitement de l'incident sont utilisées pour informer et former les collègues, et servent de documents de référence pour de futurs incidents similaires.

Les organisations humanitaires peuvent fonder leurs POS sur ce modèle en 5 étapes, en décrivant comment chaque étape doit se dérouler au sein de leur organisation. Ceci doit notamment inclure les fonctions, les rôles et les équipes au sein d'une organisation qui sont responsables à chaque étape du processus. Ces étapes doivent être intégrées ou étendues aux protocoles existants d'intervention en cas d'incident (p. ex. gestion des incidents de sécurité liés à l'accès humanitaire).

Dans un contexte donné de réponse humanitaire, les organisations doivent également s'engager à intégrer toute procédure conjointe de gestion des incidents au sein des structures de coordination existantes, telles que les clusters et les mécanismes de coordination inter et intra-cluster.

[7] Le Centre for Humanitarian Data fournit plusieurs sources d'orientation qui peuvent éclairer l'élaboration des POS sur la gestion des incidents liés aux données sur la **page Responsabilité des données**.

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

[9] Pour les organisations humanitaires, un exemple d'une telle classification est le **Cadre conceptuel de la Classification internationale pour la sécurité des patients (CISP)** de l'Organisation mondiale de la Santé (OMS).

[10] OMS, **Cadre conceptuel de la Classification internationale pour la sécurité des patients (CISP)**.

RECOMMANDATIONS POUR AMÉLIORER LA GESTION DES INCIDENTS LIÉS AUX DONNÉES

L'introduction ou l'amélioration de la gestion des incidents liés aux données dans les opérations humanitaires est essentielle pour une pratique liée aux données plus responsable dans le secteur. Le Centre for Humanitarian Data recommande aux organisations de concentrer leurs efforts sur les domaines suivants :

1. **Établir une interprétation commune de la gestion des incidents liés aux données**
   Utiliser un modèle de risque pour comprendre l'enchaînement d'évènements susceptibles d'entraîner des incidents pour des bureaux et des systèmes spécifiques. Identifier les principaux acteurs de menaces et les vulnérabilités des bureaux et des systèmes. Connaître les contrôles de sécurité existants et comprendre leur efficacité. Enfin, cartographier la capacité existante de gestion des incidents liés aux données et déterminer si elle est bien positionnée. Une fois que des définitions et des processus clairs ont été formulés, investir dans la sensibilisation du personnel et soutenir une culture de dialogue ouvert sur les incidents, dans laquelle le reporting proactif et la gestion des incidents sont incités, et non punis.

2. **Renforcer la capacité de gestion des incidents liés aux données**
   Prendre des mesures pour mettre en place des contrôles de sécurité afin de réduire le risque d'incidents liés aux données et partager les meilleures pratiques avec les partenaires. S'appuyer sur le travail existant dans le secteur pour combler les lacunes de gouvernance qui peuvent créer des vulnérabilités pour votre organisation. Collaborer avec les partenaires organisationnels pour mettre en place des canaux d'information autour des incidents liés aux données. Partager les vulnérabilités connues de manière contrôlée avec des homologues de confiance pour l'apprentissage inter-organisationnel.

3. **Soutenir l'apprentissage continu**
   Soutenir l'apprentissage et le développement de meilleures pratiques de gestion des incidents liés aux données en organisant des formations et des exercices basés sur des scénarios susceptibles de se produire dans différents contextes opérationnels. Ces exercices doivent avoir lieu régulièrement et peuvent même impliquer que plusieurs organisations se forment et s'entraînent ensemble. En outre, documenter les incidents réels liés aux données comme cas d'étude pour le développement interne des connaissances.

Les organisations sont encouragées à partager leur expérience dans le développement de la gestion des incidents liés aux données avec le Centre for Humanitarian Data via **centrehumdata@un.org**.

COLLABORATEUR: **UNIVERSITÉ DE YALE, JACKSON INSTITUTE OF GLOBAL AFFAIRS.**

Le **Centre for Humanitarian Data** (ci-après dénommé le « Centre »), en collaboration avec des partenaires clés, publie une série de huit notes d'orientation sur la Responsabilité des données dans l'action humanitaire au cours de 2019 et 2020. La série de notes d'orientation fait suite à la publication du **projet de directives opérationnelles sur la responsabilité des données du Bureau de la coordination des affaires humanitaires des Nations Unies** (UNOCHA) en mars 2019. Par le biais de cette série, le Centre vise à fournir des orientations supplémentaires sur des questions, des processus et des outils spécifiques pour la Responsabilité des données dans la pratique. Cette série est rendue possible grâce au généreux soutien de la Direction générale de protection civile et opérations d'aide humanitaire européennes (DG ECHO).

La traduction de ces notes a été facilitée par CartONG grâce au soutien du Ministère français de l'Europe et des Affaires Etrangères.