HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

Mini MBA Security and Risk Management: protecting teams and maintaining access

Course handout · Week 6 : Incidents: report, analyse, learn

A programme of exactly 3 months (12 weeks, 144 hours) to manage the security and risks of a humanitarian organisation: duty of care, context analysis, risk assessment, plans and procedures, acceptance and access negotiation, incidents, crisis management and kidnapping, staff health and wellbeing, digital security and data protection, organisational risks and compliance, risk sharing with partners, governance and business continuity. Corrected numerical exercises, three monthly exams with case studies, and a verifiable diploma from the Humanitarian Academy.

https://humanitairejobs.org/en/academy/mini-mba-securite-risques/semaine-6/

Free document from the Humanitarian Academy. It may be printed and shared freely for training purposes, without modification.

Week 6 : Incidents: report, analyse, learn

Objectives

- Set up an incident and near-miss reporting system that encourages information to flow upwards.
- Analyse an incident with a structured method (timeline, causes, contributing factors) without a blame culture.
- Use incident data to adjust measures and report to senior management and donors.

Why report

A **security incident** is any event that caused or could have caused harm to staff, assets, reputation or programmes. A **near miss** is an event that could have caused harm but did not: gunfire heard near a convoy, a fake checkpoint narrowly avoided, a verbal threat.

Reporting serves to:

- **provide assistance** immediately to the people affected;
- **alert** other teams and organisations;
- **understand** trends and adapt measures;
- **account** to senior management, the board, donors and insurers;
- **demonstrate** that the organisation is exercising its duty of care.

The incident pyramid (observed in many sectors) shows that before a serious incident there are generally many near misses and minor incidents. Not reporting them means depriving yourself of early warnings.

The reporting system

An effective system has three levels:

- **Immediate alert** (within the hour): a call or message to the designated person, with the essential information: who, what, where, when, condition of the people involved, need for help.
- **Incident report** (within 24 to 48 hours): a standard form with timeline, consequences, actions taken.
- **Analysis** (within 1 to 2 weeks for significant incidents): causes, lessons, recommendations.

To encourage reporting:

- a simple form, available offline and in staff languages;
- **no sanction** for reporting a good-faith error (a "just" culture, which distinguishes honest error from gross negligence or deliberate violation);
- a **confidential** channel for sensitive incidents (sexual violence, harassment, incidents involving a colleague);

- **feedback**: teams see what changes as a result of their reports.

> If a team never reports anything, it is almost never because nothing happens. It is a warning sign about the security culture.

Classifying incidents

A common **typology** makes data comparable: violence against people (murder, injury, kidnapping, sexual assault, arbitrary detention), theft and robbery, intrusion, threat, conflict-related incident (gunfire, shelling, explosive devices), road accident, health incident, digital security incident, civil unrest.

Each incident is also given a **severity level**, for example from 1 (minor, no injury or significant loss) to 4 (critical: death, kidnapping, serious injury, withdrawal from an area).

Example of a quarterly table. 42 incidents reported: 15 minor thefts, 9 threats, 6 road accidents (2 of them serious), 5 carjackings, 4 conflict-related near misses, 2 short arbitrary detentions, 1 physical assault. There are 8 incidents of severity 3 and 4, i.e. 19%. All 5 carjackings took place on the same route, between 15:00 and 17:00: the trend can be acted on (change of timings, review of authorisations on that route).

Analysing an incident

The analysis of a significant incident seeks to understand, not to punish. A four-step method:

- A precise **timeline**, reconstructed from several sources (people involved, witnesses, communications, GPS).
- **Facts and consequences**: damage, reactions, assistance provided.
- **Causes and contributing factors**: context (threat), vulnerabilities (procedures, behaviour, equipment), decisions taken and the reasons for them, what worked well.
- **Recommendations**: concrete measures, persons responsible, deadlines, and verification of their implementation.

Useful questions: was the threat known? Were the procedures appropriate? Were they known and applied? If not, why not (impossible, unknown, bypassed)? Was the response to the incident fast and appropriate? What should we have seen coming?

The people affected must be **protected** during the analysis: psychological support, respect for their pace, confidentiality, and no repeated questioning that re-traumatises them.

Using the data

Incident data feed into:

- the **context analysis** and the risk assessment (frequencies, locations, timings, perpetrators, modus operandi);
- **decisions** on measures (what works, what does not);
- **reports** to senior management (quarterly dashboard) and to the board;

- **sharing** with security forums and sector databases, in anonymised form and with the organisation's agreement.

Useful indicators. Number of incidents per 100 staff; share of serious incidents; average reporting time; share of recommendations implemented on time. **Example:** 24 recommendations from the year's analyses; 15 implemented on time, 5 late, 4 not started. On-time implementation rate: 62.5%. The 4 not started are examined as a priority by senior management: a recommendation that is not applied leaves the risk intact.

Reporting and communicating

After a serious incident, several audiences expect information, with different needs:

- The **family** of those affected: fast, humane information, from a designated person, before any public communication.
- **Staff**: factual information, measures taken, support available, to avoid rumours.
- **Donors**: depending on the contracts, rapid notification of serious incidents and their consequences for programmes.
- **Insurers**: notification within the deadlines for damage and medical costs.
- **Other organisations**: alert through the security forum.
- **Media**: only through the designated spokesperson; in the case of a kidnapping, public communication can put the victim in danger and is decided by the crisis management team.

Clumsy communication can make an incident worse: publishing a victim's name before the family has been told, publicly accusing an armed actor, or revealing information that compromises a negotiation.

Exercise: analysing a carjacking

Situation. One of the organisation's vehicles was carjacked at 16:40 on the southern route, 25 km from the base; the driver and two staff members were not injured, but the vehicle, two laptops and USD 4,000 in cash per diems were taken. Facts: the movement authorisation provided for arrival before 16:00; the distribution had been delayed; the 16:00 check-in call was not made (no network); the base manager did not trigger the missing vehicle procedure until 17:30. In the previous quarter, 3 near misses had been reported on the same route in the late afternoon, without any change to procedures. The cash per diems were being carried "to keep things simple".

Task. 1) Contributing factors. 2) What worked well. 3) Recommendations.

Answer. 1) Late departure without reassessment (curfew procedure not applied in the face of the delay); an area without network coverage and no alternative means of communication; a 90-minute delay before the missing vehicle procedure was triggered; previous near misses not acted upon; visible and unnecessary transport of cash. 2) Non-resistance by staff, with no injuries; immediate reporting after the incident. 3) A clear rule: in the event of a delay, stay on site in a safe place assessed in advance rather than driving on this route in the late afternoon; satellite phone or tracking device for areas without network coverage; missing vehicle procedure triggered no later than 15 minutes after a missed call; systematic analysis of near misses; payment of per diems by mobile money or bank transfer, and a ceiling on cash carried; psychological support for the three staff members; persons responsible and deadlines for each recommendation, monitored by the country director.

Key takeaways

- Report incidents and near misses: the base of the pyramid prevents the top.
- Three levels: immediate alert, report within 48 hours, analysis of significant incidents.
- Just culture: no sanction for an honest error that is reported; confidential channels.
- Analyse to understand: timeline, causes, contributing factors, recommendations followed up.
- After a serious incident: the family first, a single spokesperson, absolute caution in the event of a kidnapping.

Quiz

1. Gunfire heard near a convoy, with no injuries or damage, is:
   A. Nothing to report
   B. A serious incident
   C. A near miss to be reported
   D. A health incident
2. 48 incidents, 12 of them of severity 3 or 4. The share of serious incidents is:
   A. 12%
   B. 25%
   C. 36%
   D. 4%
3. 30 recommendations, 21 implemented on time. Rate:
   A. 70%
   B. 30%
   C. 21%
   D. 63%
4. In a just culture, a staff member who reports an honest error:
   A. Is sanctioned as an example
   B. Is transferred
   C. Must pay for the damage
   D. Is not sanctioned, and the error is used for learning
5. After a staff member is kidnapped, who decides on public communication?
   A. The headquarters communications department alone
   B. Each colleague on social media
   C. The crisis management team
   D. The local media

Quiz answers : 1. C · 2. B · 3. A · 4. D · 5. C