Context and Key Challenges

Using open sources, key informant interviews and data shared by response actors, Insecurity Insight has identified a heightened risk of sexual violence and abuse against civilians and local healthcare workers in the DRC. In eastern DRC, evidence on sexual violence suggests that:

- locals are at greatest risk;
- perpetrators cannot easily be held accountable;
- national and international response actors are not targets of sexual violence, but may be at heightened risk if caught up in larger security attacks; and
- local healthcare workers are at risk of sexual harassment and sexual abuse by superiors who demand sexual favours in exchange for improved work conditions.

Sexual violence is a reality in the DRC. Documenting cases can be difficult both practically and emotionally. Sexual violence is often committed during attacks on civilians. Reporting can be deeply distressing for the survivors, who have to relive the trauma and face shame and stigma.

Sexual violence is widespread among civilians in the Ebola-affected eastern regions. Armed militia groups have been known to target women and girls while they are walking to school or collecting firewood. State actors, including the armed forces and police, are also reported to have targeted individuals, including during detention in police custody.

Security Strategy

The exact reasons for incidents of sexual violence and abuse will vary from case to case. Preventing and responding to such attacks requires a combination of acceptance, protection and deterrence strategies. It is important that organisations are appropriately prepared to respond to an incident of sexual violence against or abuse of a staff member.

Response organisations can use three security strategies in humanitarian settings:

- **Acceptance** involves building a safe operating environment through the approval, consent and cooperation of communities, local authorities and other stakeholders in the operational area.
- **Protection** involves reducing risk by reducing the vulnerability of the organisation and its employees, e.g. through the use of walls, fences and armoured vehicles.
- **Deterrence** involves reducing risk by containing external threats through the use of counter-threats, e.g. obtaining armed protection and exercising diplomatic/political leverage.

Most response organisations will adopt a combination of these approaches, based on what they perceive as being appropriate to a particular setting. However, it is important to remember that the behaviour and approach of a response actor will impact future efforts to develop community acceptance, e.g. the use of armed protection.
SECURITY RISK MANAGEMENT MEASURES

While incidents of sexual violence and abuse must be considered within the framework of response organisations’ broader security risk management processes, given the sensitive nature of sexual violence cases, the implementation of prevention, preparedness and response activities requires dedicated staff, and measures and mechanisms being in place to ensure the confidentiality of the incident and the protection of the survivor. While each incident of sexual violence and abuse will be different, organisations should broadly focus on prevention, preparedness, response and post-incident measures.

Prevention
Organisations should endeavour to prevent incidents from occurring in the first place. Prevention efforts are supported by
- conducting inclusive risk assessments that assess threats outside and within the organisation (i.e. that consider the possibility of staff members being both victims and perpetrators);
- carrying out induction and training (e.g. how to take action and get support if a staff member experiences sexual violence);
- developing and implementing accessible and confidential reporting and whistleblowing mechanisms;
- developing and implementing disciplinary actions, investigations and references;
- addressing organisational cultures that promote or permit sexual violence and abuse. Organisations should promote a safe work environment and adopt a zero-tolerance policy towards sexual violence and abuse.

Preparedness
Organisations should develop policies and procedures for dealing with sexual abuse and violence; train staff to deal with these issues; and clearly assign responsibilities for first responders, survivor support and investigations.

Response and aftercare
Organisations should respond to incidents appropriately and provide aftercare. This includes:
- defining and implementing policies and guidance for sexual violence responders that outline the immediate response, the response needed within 24 hours, and actions that need to be taken within 24-72 hours;
- defining and implementing aftercare for survivors (medical, psychological and legal support), and processes for investigations.

Response organisations that experience an incident of sexual violence against or abuse of a staff member are encouraged to seek professional advice immediately. More information can be found in EISF’s guide ‘Managing Sexual Violence against Aid Workers’.

Security risk management process
To improve the security of response actors and their access to affected communities, organisations should follow a security risk management process that involves the identification of risks and implementation of mitigating measures. Broadly, this involves:
- carrying out a contextual analysis and mapping the actors in each operational area;
- assessing the risks that response actors will face in each operational area (i.e. by carrying out a risk assessment);
- identifying possible risk management measures to mitigate identified risks. These include:
  - measures that prevent the risk altogether (e.g. not operating in a given context);
  - measures that reduce the likelihood of risks occurring (e.g. implementing a curfew for healthcare responders);
  - measures that reduce the impact should an event happen (e.g. evacuation and emergency medical support);
- developing a security plan that incorporates these identified measures and provides guidance for staff on how to implement them through detailed standard operating procedures and contingency plans;
- implementing a security incident information management system through which security incidents are reported, analysed and used to inform improved security risk management measures.
FURTHER READING


OTHER DOCUMENTS IN THE SERIES

1. Introduction to delivering aid and emergency healthcare in insecure settings
2. Introduction to Security Risk Management
3. Security challenge: Non-state armed groups
4. Security challenge: Community resistance and mistrust
5. Security challenge: Arson attacks on healthcare facilities
7. Security challenge: Sexual violence and abuse

RESOURCES OFFERED BY INSECURITY INSIGHT

Mailing list
• Sign up to receive all the latest news and resources from Insecurity Insight.

Reporting platform
• Report Abuse: This is an independent online confidential platform for survivors of sexual violence and abuse in the aid workplace to record their story.

Toolkit
• This explains what the Report Abuse platform is, who it is for, and how to use it. It is designed to be used by security focal points, personnel responsible for safeguarding staff well-being, and providers of training. It features talking points to support organisations’ own training programmes.

Mobile guide:
• In this ten-minute DisasterReady! mobile guide, staff learn how to take action, report an incident, and obtain support when sexual violence and abuse happens to them or a colleague.

Datasets
• Sexual Violence and Abuse in the Aid Workplace: This dataset contains verified submissions from Aid in Danger partner agencies and open-source data on sexual violence against and the abuse of aid workers between January 2015 and December 2017.

Report
• Monthly News Briefs: These provide briefings on safety, security and access incidents that affect healthcare workers, infrastructure and services around the world. They are compiled from open sources with links to the original information where possible, and provide a summary of WHO SSA-reported events.