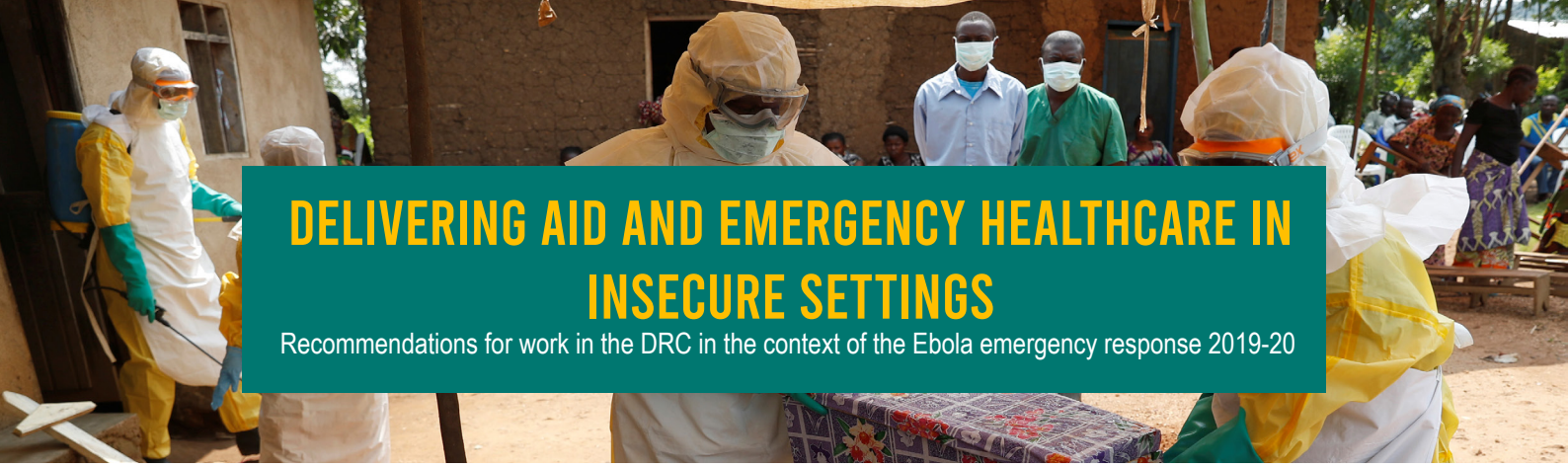

DELIVERING AID AND EMERGENCY HEALTHCARE IN INSECURE SETTINGS

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

INTRODUCTION

In the Democratic Republic of the Congo (DRC), over **2,200 people have died of Ebola** since August 2018. According to **data** gathered through open sources and direct reporting to Insecurity Insight by response actors throughout 2019, at least 20 responders died violent deaths during attacks in the eastern part of the country and at least 16 were abducted. Forty-three healthcare facilities were burnt down and 248 threats against response actors were considered serious enough to be documented and reported. Although no quantitative data is available on incidents of sexual violence and abuse, informants highlight a heightened risk of this type of violence against national response actors.

These figures exemplify the challenges of rolling out an emergency response in areas outside of government control where the healthcare system is weak, ongoing conflict is under way, and historical tensions exist between local communities and the central government. The data and contextual dynamics particularly highlight the complexities of gaining community acceptance in areas affected by conflict and where armed groups maintain control over territories.

THE CONTEXT AND RESPONSE

Prolonged conflict has plagued eastern DRC for more than 20 years. Humanitarian actors have carried out healthcare activities in the country for many years. Local health structures are not aligned with the national healthcare system, which is itself fractured. Throughout the DRC, many specialised and externally funded disease control programmes are administered through their **own programme structures**.

However, compared to the 2013-16 Ebola outbreak in West Africa, the 2018-19 DRC Ebola response benefits from improved tools and medical management of the epidemic, such as newly developed treatments, including a vaccine. Many of the Ebola treatment centres are also more open and accessible to patients' families. These benefits, however, are often adversely affected by significant contextual challenges. Most significantly, rumours that fuelled widespread negative perceptions of the response and the actors involved have made it difficult to gain community acceptance. The belief is not uncommon that outsiders, including foreigners and Congolese responders who do not belong to the affected communities, have fabricated the outbreak for their **political or economic benefit or to further destabilise** the region.

The use of **inaccessible technical language** has also not helped to alleviate fears and suspicions. Furthermore, the presence of outsiders has affected the power relations and economic interests of actors in eastern DRC, including local businesses and armed groups, further causing tensions internally among these interest groups and externally with foreign actors.

The difficulties of rolling out the emergency response have also had negative consequences for the overall healthcare system in eastern DRC. Local healthcare workers have been pulled away from general healthcare provision into better-paid Ebola response roles,[5] and routine healthcare interventions – such as vaccination campaigns – have been put on hold or delayed as attention and resources are diverted to the complex fight against Ebola.

In 2019, **4,000 people died of measles** in the DRC, three times the number of cases reported in 2018. Moreover, the frequent attacks on healthcare providers have not only caused personal tragedies for victims' families, but have also resulted in the **withdrawal of health services** for security reasons. This will have long-term impact on the population in eastern Congo's overall access to healthcare, and also has implications beyond the Ebola healthcare response. The consequent risk of disease transmission and the increasing insecurity due to the region's changing conflict dynamics have also affected the whole aid sector in the affected areas. Projects not directly concerned with healthcare have also been required to monitor the situation and adapt their strategies.

SECURITY CHALLENGES FACED BY RESPONSE ACTORS

Research conducted by Insecurity Insight indicates that response actors in the DRC are currently facing several significant challenges that could result in direct and indirect consequences for their security. These include:

1. **insecurity due to ongoing conflict and the presence of non-state armed groups;**
2. **community resistance due to mistrust of the response and response actors;**
3. **insecurity in the form of arson attacks on healthcare facilities;**
4. **the heightened risk of abduction facing national responders;**
5. **the risk of national responders becoming victims of sexual violence and abuse.**

RECOMMENDATIONS

This document provides practical recommendations for implementing appropriate security risk management measures in eastern DRC to enable response actors, including healthcare workers, to effectively address the security challenges highlighted in the previous section.

These recommendations are based on information collected from open sources and through key informant interviews, and data reported directly to Insecurity Insight by response actors.

The evidence collected suggests that security risk management measures implemented in eastern DRC should adopt an approach that focuses on adherence to core humanitarian principles in order to gain the acceptance of local communities and actors, i.e. an acceptance approach.

The recommendations shared by Insecurity Insight, therefore, focus on a strategy to gain the acceptance of community members and armed groups, as well as practical recommendations on ways to prevent and respond to the abduction of response actors, incidents of sexual violence, and arson attacks on healthcare facilities.

The practical recommendations respond directly to the concerns identified in Insecurity Insight's **trend analysis of attacks**, which followed the **biweekly monitoring** of reported attacks on healthcare staff and facilities between September and November 2019 as part of the H2H response activity supported by UK aid from the UK government.

These recommendations use a security risk management framework and are designed for practitioners engaged in planning, management, operations, and policy development in conflict-affected territories in DRC. This includes practitioners working at headquarters and field levels of multilateral institutions, governments in affected countries, and national or international non-governmental organisations involved in the response.

Security risk management framework

A security risk management framework supports response actors, including healthcare providers, in their efforts to translate their duty-of-care obligations into key processes and actions that will not only enhance staff security, but also improve their organisations' reputation and credibility. A good security risk management framework enables the effective day-to-day management of security risks and events. To learn more, see: www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS

SECURITY RISK MANAGEMENT

Improving the security and access of response actors, including healthcare workers, through effective security risk management based on humanitarian principles

Humanitarian security risk management allows greater access to and impact for crisis-affected populations through the protection of aid workers, programmes, and organisations.

WHAT IS SECURITY RISK MANAGEMENT?

Security risk management refers to the day-to-day management of security risks. Effective security risk management can address operational challenges that impede healthcare actors' access to communities in need.

All organisations and health service providers have a duty of care towards their staff. This means ensuring that appropriate mitigation measures and support are in place to prevent and respond to security incidents. All staff should be adequately informed of the risks they face in their work and the mitigation measures put in place by their employer. The higher the levels of insecurity, the greater the responsibility that response organisations have towards mitigating the risks faced by their staff.

Programmes and healthcare and administrative staff at all levels have a collective responsibility to manage and reduce risks when they are working in insecure environments.

Good security risk management involves:

- ensuring that security is addressed and clarified in the organisational structure and descriptions of staff responsibilities;
- ensuring that security policies are in place and security requirements are clear to all staff;
- carrying out regular context analyses and risk assessments;
- implementing security plans based on identified risks;
- putting in place security arrangements and support in order to prevent, prepare for, and respond to identified risks;
- ensuring that staff who travel as part of their work are aware of and prepared for potential risks;
- informing and training staff on security risks and their responsibilities with regard to mitigating these risks;
- reporting and learning from security incidents;[2]
- preparing and responding to critical incidents by developing an appropriate crisis management structure and plan;
- collaborating with other organisations to share information on incidents, context analyses and good practice in security.

To learn more, see EISF's guide: 'Security risk management: a basic guide for smaller NGOs' and ODI's good practice review 'Operational security management in violent environments'.
For practical steps on how to improve security at field level, see EISF's 'Security to go' guide.

By improving the security of response actors, organisations are also improving these actors' access to affected communities.

SECURITY RISK MANAGEMENT IN THE EBOLA RESPONSE

Although the Ebola virus is undoubtedly a public-health concern, the outbreak in eastern DRC is part of a broader complex emergency in which historical and present-day conflicts, a weak national healthcare system, and other humanitarian concerns interact to intensify the spread of Ebola and cause further humanitarian issues. Similar complex emergencies have occurred in other settings such as Yemen and Iraq. Lessons from these contexts indicate that responders must approach the situation as a complex emergency requiring a concerted humanitarian response, not purely an Ebola-focused healthcare intervention. Framing an emergency response healthcare intervention in conflict-affected areas according to humanitarian principles **helps to gain community members'** acceptance and increase responders' access to affected communities.

To effectively manage staff security in a complex emergency, responding organisations should focus particularly on adopting what we call an "acceptance approach" to security or an "acceptance strategy". An acceptance approach/strategy fosters local trust and ownership of the response. In the DRC, this involves implementing several important measures within a broader security risk management framework.

Acceptance strategy

An acceptance strategy/approach to security attempts to reduce or remove threats posed by external actors to response activities and personnel through the building of relationships with local communities and other stakeholders in the areas of operation. This particularly involves obtaining their **acceptance of and consent** for the response actors' presence and work.

To obtain community and other stakeholders' acceptance of their activities, response actors should adhere to core humanitarian principles, which serve to reassure local communities about the purpose of response activities and the code of conduct that response actors commit to adhere to.

Humanitarian principles

The core humanitarian principles provide a normative basis to guide humanitarian interventions in conflict-affected areas and can help ensure acceptance by affected communities and both state and non-state armed groups. The **core humanitarian principles**, as defined by UNOCHA, are:

- **Humanity:** Human suffering must be addressed wherever it is found. The purpose of humanitarian action is to protect life and health and ensure respect for human beings.
- **Neutrality:** Humanitarian actors must not take sides in hostilities or engage in controversies of a political, racial, religious or ideological nature.
- **Impartiality:** Humanitarian action must be carried out on the basis of need alone, giving priority to the most urgent cases of distress and making no distinctions on the basis of nationality, race, gender, religious belief, class or political opinions.
- **Independence:** Humanitarian action must be autonomous from the political, economic, military or other objectives that any actor may hold with regard to areas where humanitarian action is being implemented.[5]

The recommendations developed by Insecurity Insight provide specific security measures that foster an acceptance strategy/approach by drawing on and adhering to core humanitarian principles in order to address some of the security challenges currently faced by response actors, including healthcare workers, operating in the DRC.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS

SECURITY CHALLENGE: NON-STATE ARMED GROUPS

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

In March, suspected ADF forces burnt down a health clinic and several houses during an attack on Lubwasi town. Six civilians were also killed by guns or machetes, and several houses in the area were burnt down.

CONTEXT AND KEY CHALLENGES

Using open sources, key informant interviews and data shared by response actors, **Insecurity Insight** has identified the following contextual challenges relating to the presence and involvement of non-state armed groups in response areas of operation that have impacted both response actors' security and their access to affected communities.

- During the first six months of 2019, armed groups carried out over 550 attacks on civilians. In some of these attacks **healthcare facilities were burnt down or staff members were killed or abducted**.
- Some attacks directly targeted healthcare workers or facilities. Other attacks targeted a whole town and, therefore, healthcare workers were among the affected civilians and healthcare facilities among the looted properties.
- Over 100 armed groups, including Mai Mai militia and ADF forces, operate in Ebola-outbreak areas. There are tensions and competitions between the various armed groups.
- Boundaries between armed groups and state actors can be fluid and motives are not always clear. Soldiers serving with the state's armed forces can also be active armed group members. Criminal acts can be perpetrated by both armed groups and soldiers. Medical equipment or drugs may be looted to supply an armed group with needed medical care.
- Armed groups can be embedded within local communities or have close relations with them, and may share community perceptions that the Ebola crisis was artificially created to profit elites.
- Armed groups tend to have economic interests to sustain themselves.

SECURITY STRATEGY

While every organisation should adopt a combination of security strategies in accordance with the contextual dynamics of the area in which it operates, in terms of the DRC Ebola response evidence gathered by Insecurity Insight from open sources, key informant interviews and data from response actors **suggests that a strong emphasis should be placed on adopting an acceptance approach to security.**

This approach should aim to encourage non-state armed groups to accept the presence and work of response actors. An acceptance strategy can be successful in engaging armed groups to provide constructive support. Some non-state armed groups have been known to intervene with local communities on behalf of response actors, and to facilitate access to these communities when they (i.e. the armed groups) have accepted the response actors' presence and work.

Geneva Call's Deed of Commitment

In the Deed of Commitment, armed groups publicly commit to maintaining and providing access for affected populations to essential healthcare facilities, goods and services, without adverse distinction, and to facilitating the provision of healthcare by impartial and neutral humanitarian organisations. Current signees: **Alliance of Patriots for a Free and Sovereign Congo (APCLS)**.

SECURITY STRATEGY

To effectively implement an acceptance strategy, the following points apply:

- Adherence to the principles of neutrality, impartiality and independence is key.
- Response actors who appear biased towards one group can inflame a volatile situation.
- Transparency and open dialogue are important to avoid the perception by non-state armed groups that response actors are spying or otherwise trying to undermine their authority in the operational context in which these groups operate.
- Any practices that could be perceived as profiting from the delivery of healthcare services or other humanitarian activities should be avoided.
- The use of armed escorts should be carefully considered. In some contexts, using them can increase security risks and may incite attacks or cause response actors to be distrusted.

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.[1]

SECURITY RISK MANAGEMENT MEASURES

In the DRC Ebola response, response actors are encouraged to consider the following when developing their security plans and implementing security measures to deal with threats posed by non-state armed groups:

- Carry out regular contextual analysis and map the actors in each operational area. This is particularly important in eastern DRC, where rival armed groups and shifting power dynamics have a significant effect on response actors' security and access to communities.
- Be aware of how responders' activities are perceived and adopt a strategy of proactively influencing perceptions. This can be achieved, for example, through adhering to joint principles of engagement, adhering to humanitarian principles, and clearly and assertively communicating the role and objectives of response actors.
- Explore and develop interventions that are specific to the operational area. The needs and understandings of one non-state armed group can vary from that of another. This is true for community members as well. Avoid copying strategies blindly from other contexts.
- Develop strategic partnerships and/or positive relationships with other response actors, local communities, and state security forces and non-state armed groups.
- Establish and maintain transparent and consistent relations with armed actors. Long-term presence in the community, reach and communication are key.
- Where necessary, distance a health programme or other humanitarian activity from actors not perceived as neutral, in order to strengthen reach and independence.
- Be contactable.

SECURITY RISK MANAGEMENT MEASURES

- Coordinate with other response actors to overcome challenges to community access. Adherence to joint principles of community engagement can improve communities' and non-state armed groups' perception of response actors. Failure by one response actor to collaborate and adhere to principles can have knock-on effects on all response actors and severely curtail community access and staff security.
- Adopt a clearly defined vision of what health and other humanitarian interventions are working to achieve and clearly communicate the objectives and priorities of interventions in a way that it is well understood.
- Ensure that stakeholders from the local community, the government and non-state actors are engaged before commencing outreach work. There are examples in the DRC of non-state armed groups positively engaging with local communities on response issues on behalf of response actors.
- Be transparent about funding sources and objectives. Where this is possible and appropriate, maintain an open dialogue with armed groups about the organisation's activities and objectives, especially in areas where organisations work simultaneously with multiple rival armed groups.
- Conduct staff training to develop staff skills and capacity, especially in the areas of communication and negotiation with armed groups.
- Learn from security incidents. A strong security incident information management system can help organisations to understand the circumstances surrounding security incidents and support them with ongoing context analyses and risk assessments. For example, a robust incident report following an incident involving an armed group can support in-depth analysis of the cause and consequences of the incident and inform future engagement in the area and/or with that armed group.

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

Geneva Call: www.genevacall.org/wp-content/uploads/2019/07/GC-Negotiation-of-humanitarian-access-in-NK_EN2.pdf

ICRC: www.icrc.org/en/doc/assets/files/review/2011/irrc-883-schneckener.pdf

International Law: www.armedgroups-internationallaw.org/2019/02/18/engaging-armed-non-state-actors-on-the-protection-of-health-care-some-promising-steps/

RefWorld: https://www.refworld.org/pdfid/57e92e4d4.pdf

CSIS: htthttps://www.csis.org/analysis/north-kivus-ebola-outbreak-day-90-what-be-done

CSIS: :/www.csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/120125_Rubenstein_ProtectionOfHealth_Web.pdf

https://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf

AWSD: www.aidworkersecurity.org/sites/default/files/AidWorkerSecurityReport_2013_web.pdf

EISF: www.eisf.eu/news/community-mistrust-why-the-drcs-ebola-epidemic/

RECOMMENDATIONS

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**
6. **Security challenge: Abduction of health workers**
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.

Reports

- *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.
- *Attacks on Health Care in the Context of the Ebola Response*: This provides an overview of reported verified submissions from Insecurity Insight partner agencies and open-source incidents affecting the delivery of healthcare in the DRC in 2019.

Datasets

- *Attacks on Health Care in the DRC during the Ebola Response*: This dataset contains verified submissions from Aid in Danger partner agencies and open-source data on incidents affecting the delivery of healthcare in the DRC between January 2018 and November 2019.

Podcasts

- *Humanitarian Incidents podcasts*: These constitute a series of conversations with experts discussing how to understand, manage and use information on incidents, and how this can improve organisations' risk management procedures and access to crisis-affected populations. Developed together with EISF and RedR UK.

Handbook

- *Security Incident Information Management (SIIM):* This guidance handbook and tool kit shares best practice, guidelines, tools and recommendations to enhance organisational security incident information management. Developed together with EISF and RedR UK.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS

SECURITY CHALLENGE: COMMUNITY DISTRUST AND RESISTANCE

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

In February, an Ebola response team member was assaulted and injured when local residents clashed with healthcare workers after the transfer of an Ebola case to Tako village in Beni territory, North Kivu.

CONTEXT AND KEY CHALLENGES

Using open sources, key informant interviews and data shared by response actors, **Insecurity Insight** has identified the following contextual challenges relating to community distrust and resistance to the response, which have in turn impacted response actors' security and access to affected communities:

- Reports of community members threatening staff members during programme activities are frequent, and often lead to **assaults and injuries**. In many of these incidents staff members are targeted directly.
- Intimidation, threats and violence were frequently reported between February and May and in October 2019 and coincided with intensified intervention efforts due to the increase in reported Ebola cases in Katwa and Butemo, North Kivu.
- In communities in eastern DRC there are widely held local views that the Ebola outbreak was fabricated to benefit business-owning local elites or to further destabilise the region.
- Distrust in vaccinations and treatments affects the willingness of some communities to seek help from healthcare centres.
- Violence and threats affect staff well-being and their ability to provide care. This has also resulted in staff shortages.
- The use of local healthcare staff in the Ebola response can reduce the availability of healthcare staff for other interventions that communities consider to be important.
- Efforts to contain the spread of Ebola are being hampered by widespread community mistrust and resistance to outside help.

SECURITY STRATEGY

Despite the complexities of navigating through different local communities with diverse customs and languages in eastern DRC, which is an area marked by decades of conflict and poverty, the international experience of the 2013-16 Ebola response in West Africa may provide some indications of how local communities can be transformed into proactive partners to tackle Ebola. **An acceptance approach that includes a strong focus on the local community as an active response partner is key not only for access to communities, but also for the security of response actors.**

SECURITY STRATEGY

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.[1]

SECURITY RISK MANAGEMENT MEASURES

In the DRC Ebola response, response actors are encouraged to consider the following community engagement activities when developing their security plans and implementing security measures:

- Train all response staff how to effectively conduct community outreach and communicate with community members to build their trust in and acceptance of response actors and activities. Consent from community members is needed to ensure access and improve response actors' security.
- Recruit and train local community members to help build local capacity and support the sustainability of response activities without unduly diverting attention and resources away from other healthcare and humanitarian issues.
- Listen to the needs and concerns voiced by community members. Use the behavioural data collected and analysed by social science research initiatives such as the **Social Science in Humanitarian Action Platform** and the UNICEF-led **Cellule Analyses Sciences Sociales** (CASS) to inform programmatic and security risk management decisions.
- Run regular focus group discussions, dialogue sessions and workshops with community members, particularly prior to entering a community.
- Provide a free, anonymous phone number for community members to report concerns or ask Ebola-related questions. This was successfully implemented in the West African Ebola response.
- Adapt local rituals to the needs of the response so that they remain acceptable to local communities while still meeting health standards. Specialist **anthropologists and social scientists** can help organisations to adapt their response to local cultural norms.
- Respond to other health and humanitarian needs as well as Ebola to help gain local community trust and acceptance. Local communities have cited security and chronic health concerns as being of particular importance to them, and responders' failure to address these concerns can cause resentment, access constraints and insecurity. Ensure that other health interventions are maintained, particularly those related to other communicable diseases and those that are particularly important to local communities such as maternity and pediatric services and healthcare after accidents and during emergencies.

SECURITY RISK MANAGEMENT MEASURES

- Adapt information campaigns to local linguistic and social contexts; keep messages consistent and communicate them clearly.
- Be flexible during response activities and health interventions. Because every community in eastern DRC will be different, do not use a fixed community approach.
- Carry out information campaigns that involve two-way dialogue. Carry out house-by-house leaflet drops and mobilise local radio stations. These efforts must be complemented by others that provide community members with the opportunity to discuss their concerns and ask questions.
- Engage local leaders. Community members often trust local leaders more than those at the national or international level. Individuals with Ebola symptoms may first seek advice from pastors or local leaders before going to specialised Ebola treatment centres.
- Train field staff to deal with communication and language issues and to effectively engage in challenging conversations with community members. Provide guidance on how staff should speak with non-specialist audiences; role-play how to answer difficult questions and respond to hostility from community members. Disseminating this guidance and conducting appropriate training can be challenging, given the complexity of the response and the number of responders involved. Creative and rapid ways of building capacity need to be developed.
- Collaborate with community members to develop the joint ownership of programmes. Provide the community with the tools necessary to be the main front line against Ebola. A way of ensuring that communities are able to take ownership is by recruiting and training members of local communities in order to build local capacity. In the DRC, locals are already playing an important role in contact tracing. The establishment of ad hoc decision-making bodies or boards comprising responders and representatives of local communities is a positive step towards greater community ownership of response activities, with positive implications for responders' access to communities and security.

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

The New Humanitarian: www.thenewhumanitarian.org/opinion/2019/12/03/ebola-epidemic-Congo-language-communication
Geneva Call: www.genevacall.org/wp-content/uploads/2019/07/GC-Negotiation-of-humanitarian-access-in-NK_EN2.pdf
ICRC: www.icrc.org/en/doc/assets/files/review/2011/irrc-883-schneckener.pdf
https://armedgroups-internationallaw.org/2019/02/18/engaging-armed-non-state-actors-on-the-protection-of-health-care-some-promising-steps/
RefWorld: www.refworld.org/pdfid/57e92e4d4.pdf
CSIS: www.csis.org/analysis/north-kivus-ebola-outbreak-day-90-what-be-done
CSIS: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/120125_Rubenstein_ProtectionOfHealth_Web.pdf
Acceptance Research: https://acceptanceresearch.files.wordpress.com/2012/01/acceptance-toolkit-final-for-print-with-notes.pdf
AWSD: https://aidworkersecurity.org/sites/default/files/AidWorkerSecurityReport_2013_web.pdf
EISF: www.eisf.eu/news/community-mistrust-why-the-drcs-ebola-epidemic/

RECOMMENDATIONS

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**
6. **Security challenge: Abduction of health workers**
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.

Reports

- *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.
- *Attacks on Health Care in the Context of the Ebola Response*: This provides an overview of reported verified submissions from Insecurity Insight partner agencies and open-source incidents affecting the delivery of healthcare in the DRC in 2019.

Datasets

- *Attacks on Health Care in the DRC during the Ebola Response*: This dataset contains verified submissions from Aid in Danger partner agencies and open-source data on incidents affecting the delivery of healthcare in the DRC between January 2018 and November 2019.

Podcasts

- *Humanitarian Incidents podcasts*: These constitute a series of conversations with experts discussing how to understand, manage and use information on incidents, and how this can improve organisations' risk management procedures and access to crisis-affected populations. Developed together with EISF and RedR UK.

Handbook

- *Security Incident Information Management (SIIM):* This guidance handbook and tool kit shares best practice, guidelines, tools and recommendations to enhance organisational security incident information management. Developed together with EISF and RedR UK.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS

SECURITY CHALLENGE: ARSON ATTACKS

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

In February in Butembo city, where mistrust in aid workers and rumours about treatment are rampant, unidentified perpetrators set vehicles and parts of an MSF-run Ebola treatment centre on fire, destroying medical wards and equipment, and leaving four patients missing.

CONTEXT AND KEY CHALLENGES

Using open sources, key informant interviews and data shared by response actors, **Insecurity Insight** has identified a heightened risk of arson attacks against healthcare facilities in Ebola-affected areas of the DRC, with implications for response actors' security and access to affected communities.

- More than **40 reports of arson attacks on healthcare facilities** in the DRC were reported in 2019.
- The number of reported arson attacks was particularly high between February to May and in October and occurred during wider assaults on the area by armed groups and in areas characterised by community mistrust of Ebola relief efforts.
- Arson attacks are a common security threat facing healthcare facilities in Africa. In 2018, arson attacks on healthcare facilities were also reported in ten other countries, including Nigeria (by Boko Haram) and Cameroon (by Cameroonian forces).

SECURITY STRATEGY

The exact reasons for arson attacks on healthcare facilities are unclear, but they are possibly caused by community members' or other stakeholders' mistrust of and resentment towards response actors, or are part of a larger strategy by particular stakeholders to undermine response activities for political, economic or other reasons.

Preventing such attacks requires better communication and engagement with potential perpetrators, including local communities and non-state armed groups. But this is not always possible. Therefore, organisations are encouraged to adopt a combined approach to address this risk. Such an approach could include, for example, engaging in acceptance activities to improve local community and other stakeholder acceptance of and consent to response actors' presence and work. Organisations should also aim to implement protection measures to reduce the vulnerability of healthcare and other response facilities to arson attacks.

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.[1]

SECURITY RISK MANAGEMENT MEASURES

In the DRC Ebola response, response actors are encouraged to consider developing security plans and implementing security measures that prepare response actors for the threat of arson attacks on response facilities and provide guidance on how to respond in the event of an attack:

- Appoint fire warden(s) to develop and implement an evacuation plan.
- Identify an appropriate and secure alternative location to house patients and staff.
- Consider taking out insurance policies and medical coverage.
- Conduct regular inspection, monitoring, and maintenance of the site and fire-extinguishing system.
- Carry out fire evacuation and equipment training, and hold regular drills on accessing primary and secondary safe areas.
- Provide first-aid supplies to treat burns, and train staff on how to use these supplies.
- Engage and manage relations with local agencies (fire fighters, security forces) to better understand their capacity for intervention.
- Draw up a crisis management plan and pre-identify members of a crisis or incident management team that can provide support by coordinating emergency medical and psychological care for affected staff and patients, contacting and liaising with family members of affected individuals, coordinating the relocation and/or evacuation of staff, managing media and communications, and managing all the other issues relating to the incident.
- Assess the impact of the organisation's withdrawal following a severe attack and develop an appropriate and secure exit strategy should the organisation deem programme closure or temporary withdrawal necessary following a severe incident.

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

EISF: www.eisf.eu/wp-content/uploads/2017/04/EISF_Security-to-go_guide_Module-7_Security-of-facilities-2nd-ed.pdf
EISF: www.eisf.eu/library/office-closure-eisf-guide/
EISF: www.eisf.eu/library/crisis-management-of-critical-incidents/

RECOMMENDATIONS

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**
6. **Security challenge: Abduction of health workers**
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.

Reports

- *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.
- *Attacks on Health Care in the Context of the Ebola Response*: This provides an overview of reported verified submissions from Insecurity Insight partner agencies and open-source incidents affecting the delivery of healthcare in the DRC in 2019.

Datasets

- *Attacks on Health Care in the DRC during the Ebola Response*: This dataset contains verified submissions from Aid in Danger partner agencies and open-source data on incidents affecting the delivery of healthcare in the DRC between January 2018 and November 2019.

Podcasts

- *Humanitarian Incidents podcasts*: These constitute a series of conversations with experts discussing how to understand, manage and use information on incidents, and how this can improve organisations' risk management procedures and access to crisis-affected populations. Developed together with EISF and RedR UK.

Handbook

- *Security Incident Information Management (SIIM):* This guidance handbook and tool kit shares best practice, guidelines, tools and recommendations to enhance organisational security incident information management. Developed together with EISF and RedR UK.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS

SECURITY CHALLENGE: ABDUCTION OF HEALTH WORKERS

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

In September 2019, suspected Mai Mai militia entered a hospital in Mususa commune, Butembo, and kidnapped a doctor and two nurses. The doctor was reportedly tortured and threatened with death in retaliation for collaborating with Ebola responders.

CONTEXT AND KEY CHALLENGES

Using open sources, key informant interviews and data shared by response actors, **Insecurity Insight** has identified a heightened risk of the abduction of healthcare workers in the DRC.

- In 2019, at least **14 healthcare workers were abducted** in the DRC.
- Abductions occurred while individuals travelled to and from intervention sites, at healthcare facilities or during wider assaults on the area.
- The majority of abductions took place in North Kivu.
- Many healthcare workers in the area work in constant fear of abduction and physical harm.
- Around half of those who were abducted were released within a few hours.
- The status of at least four healthcare workers remains unknown.

SECURITY STRATEGY

The exact reasons for abductions will vary from case to case. However, some abductions may be motivated by community or other stakeholders' mistrust of and resentment towards response actors, or are part of a larger strategy by particular stakeholders to undermine response activities for political, economic or other reasons.

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 the possible abduction 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.[1]

SECURITY RISK MANAGEMENT MEASURES

In the DRC Ebola response, response actors are encouraged to include the risk of abduction of healthcare workers and other national staff members in their security plans.

Be aware that each abduction incident will be different and will require a unique response. Responding to an abduction incident is a very sensitive and complex process that requires a professional intervention and the involvement of experienced and trained individuals. However, organisations should take the following steps, as appropriate:

- Carry out regular contextual analyses and map local actors in order to understand the role of the various actors in the operational area and the power dynamics involved.
- Conduct a risk assessment to understand the risk of abduction, including likely targets, in a specific operational area. To date, abductions in the DRC have targeted national healthcare workers and predominantly taken place in North Kivu.
- Develop positive relationships with local stakeholders, including community members, local leaders and others. The acceptance and support of these local authorities can sometimes be crucial to preventing abductions in the first instance. These local authorities can also play a crucial role in supporting the positive resolution of an abduction incident should one occur.
- Plan and prepare for the possible abduction of a staff member by developing a crisis management plan that clarifies the crisis management structure, and policies and procedures to be followed in the event of an incident.
- Manage an incident from initial response through to the incident's resolution or closure. The security of information in an abduction incident is particularly important.
- Manage post-incident activities, including aftercare for affected individuals.

Response organisations that experience a staff abduction are encouraged to seek professional advice immediately. More information can be found in EISF's guide '**Abduction and Kidnap Risk Management'.**

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

Geneva Call: www.genevacall.org/wp-content/uploads/2019/07/GC-Negotiation-of-humanitarian-access-in-NK_EN2.pdf
ODI: www.odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf
Devex: www.devex.com/news/minimizing-aid-worker-risk-in-dangerous-environments-94446\
ReliefWeb: www.reliefweb.int/report/world/humanitarian-groups-seek-ways-reduce-attacks-aid-workers
EISF: www.eisf.eu/wp-content/uploads/2014/09/0120-Buth-EISF-2010-Abduction-management.pdf
AWSD: www.aidworkersecurity.org/sites/default/files/AidWorkerSecurityReport_2013_web.pdf

RECOMMENDATIONS

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
6. Security challenge: Abduction of health workers
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.

Reports

- *Aid Workers Kidnapped*: This offers an overview of reported verified submissions from Insecurity Insight partner agencies and open-source incidents of aid worker kidnappings and highlights the key trends in 2018..
- *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.
- *Attacks on Health Care in the Context of the Ebola Response*: This provides an overview of reported verified submissions from Insecurity Insight partner agencies and open-source incidents affecting the delivery of healthcare in the DRC in 2019.

Datasets

- *Attacks on Health Care in the DRC during the Ebola Response*: This dataset contains verified submissions from Aid in Danger partner agencies and open-source data on incidents affecting the delivery of healthcare in the DRC between January 2018 and November 2019.

Podcasts

- *Humanitarian Incidents podcasts*: These constitute a series of conversations with experts discussing how to understand, manage and use information on incidents, and how this can improve organisations' risk management procedures and access to crisis-affected populations. Developed together with EISF and RedR UK.

Handbook

- *Security Incident Information Management (SIIM):* This guidance handbook and tool kit shares best practice, guidelines, tools and recommendations to enhance organisational security incident information management. Developed together with EISF and RedR UK.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS

SECURITY CHALLENGE: SEXUAL VIOLENCE AND ABUSE

Recommendations for work in the DRC in the context of the Ebola emergency response 2019-20

All response activities relating to sexual violence and abuse should be survivour-centred. This means that the survivor has control over all decisions relating to the incident. The only exception to this approach would be if the survivor's wishes place the survivor or others at risk of harm.

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.[1]

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

EISF: www.eisf.eu/wp-content/uploads/2019/03/2307-EISF-March-2019-Managing-Sexual-Violence-against-Aid-Workers.pdf
UN: www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2019/discussion-paper-what-will-it-take-promoting-cultural-change-to-end-sexual-harassment-en.pdf?la=en&vs=1714

RECOMMENDATIONS

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
6. Security challenge: Abduction of health workers
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.

This document was produced by **Insecurity Insight** as part of the **H2H Network** DR Congo Ebola response activation and has been funded by the H2H Fund, which is supported by aid from the UK government. This information is part of the general data collection activities carried out by Insecurity Insight in support of the **Safeguarding Health in Conflict Coalition (SHCC)** and the **Researching the Impacts of Attacks on Healthcare Project (RIAH)**. It is supported by the **Department for International Development (DFID)** of the UK government. Image: Goran Tomasevic/REUTERS