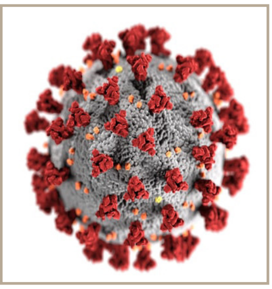
# SECURITY CHALLENGE: MOB ATTACKS

Recommendations for protection of medical facilities against a mob attack.



## CONTEXT AND CHALLENGES

It is extremely difficult to protect a facility under attack from an angry mob. Most health facilities are designed to be open to the public and welcoming. This makes health facilities easy targets that are difficult to protect even with security measures in place. There are, however, a few measures that can be considered to pre-empt and prepare for mob attacks.

In the majority of cases, a mob that is seeking justice, will not be armed with formal weapons but will vent their anger by sheer number of people using improvised weapons. In war and conflict zones, however, there is a high likelihood that attackers will carry firearms and/or explosives.

## SECURITY APPROACH

Those managing health facilities should focus their efforts on:

- Prevention/protection: protecting health facilities from mob violence, for example, by implementing an acceptance strategy to reduce the likelihood of your facility and staff becoming targets, and increasing the security of your facility.
- Preparedness and response: putting in place measures to prepare the facility and staff in the event of an emergency, for example, emergency contacts, first aid kits and evacuation routes to support staff with responding to an incident of mob violence.

The following sections go into detail on actions that can be taken to prevent, prepare for and respond to a mob attack.

## SECURITY STRATEGY

The exact reasons for mob attacks on health care facilities vary. Reasons include community members' or other stakeholders' mistrust of and resentment directly towards health care providers or as a symbol for wider frustrations related to governments or other power structures. Some may be organised by a variety of actors as part of a larger strategy to undermine response activities for political, economic or other reasons.

In the context of the COVID-19 response, some attacks may also be a spontaneous outburst of anger triggered by COVID-19 prevention measures implemented by state authorities and where the health facility acts as a symbol for such interventions and a physical structure at which to target frustrations.

Preventing such attacks requires ongoing communication and engagement with potential perpetrators, including local communities, non-state armed groups as well as state authorities enforcing general public health measures. But this is not always possible.

Health care providers may be best advised 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. Health care providers should also implement protection measures to reduce the vulnerability of health workers to mob 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.**

# SECURITY RISK MANAGEMENT MEASURES

Health facilities may consider developing security plans and implementing security measures that prepare response actors for the threat of mob attacks on response facilities and provide guidance on how to respond in the event of an attack.

**The main risks to be considered are:**

- **Fire and arson**
- **Throwing of rocks**
- **Attacks on vehicles**
- **Attempts to enter the premises**
- **Physical attacks on health workers or clients (and their families)**
- **Intimidation of health workers and spreading fear.**

To counter these main risks, the following measures can be considered:

## A COMMUNITY ACCEPTANCE STRATEGY

The core source of organisational safety and security comes from the community. This is achieved through regular community liaison, ideally weekly meetings, to gain an understanding of community perceptions of the health programme, services delivered and any potentially negative areas that need to be improved upon to enhance acceptance.

Such a strategy can be further assisted by organising regular visits to the facility by key stakeholders such as religious leaders, community representatives, schoolteachers, etc.

## COMPOUND AND ORGANISATIONAL ASSESSMENT

A security risk assessment of the entire facility focusing on:

- Location, characteristics and layout of the facility.
- Evaluation of the facility's physical protection system.
- Site survey to promote swift threat detection, delay and response.
- Estimate performance against specific threats.

To identify vulnerabilities for people and assets, such assessments can be commissioned from companies familiar with the context and with a proven track record of providing high quality services.

**Things to consider:**

- **The perimeter and facility must be protected to detect and delay forceful entry.**
- **Access points to the perimeter and facility should be protected by steel gates that cannot be penetrated by unauthorized persons (or by vehicles).**
- **An access control system  should be in place to allow entry only to authorized persons.**
- **Any potential vulnerabilities of the perimeter and/or building should be evaluated, and appropriate actions taken, for example: securing of windows, air ventilation ducts, rooftop etc.**
- **Threat-specific emergency plans are developed and practiced periodically by all staff.**
- **Coordinate with law enforcement to ensure that, in case of emergency, they can and will respond swiftly.**
- **Collaborate with communities as well as community leaders, strengthen acceptance and build trusting relationships.**

**For more info, please see this GISF resource: gisf.ngo/resource/office-opening**

## ✓ FIRE AND ARSON

- Ensure that all buildings in your compound are equipped with fire alarms and firefighting equipment.
- Fire extinguishers should be available inside the building and fire buckets filled with water or sand placed at the outside.
- Ensure that all personnel are trained to use this equipment.
- Fuel must be stored away from buildings and vehicles.
- Store all flammable materials such as vehicle and generator fuel / gas bottles in a well locked/ventilated building.
- Have a fire evacuation plan, evacuation signs, fire wardens, and regular fire drills.

## ✓ GUARDS AND PERIMETER

- Seek to surround your premises in a non-intimidating way to separate the perimeter from its surroundings.
- Try to ensure that this wall or fence blends in with the security measures taken by surrounding compounds so that your compound does not stand out as a “fortress”.
- Have a solid entry control system in place where guards can control the flow of people entering the compound.
- Have a system in place where the main entry point can be closed off with a solid gate.
- In cases of heightened threat, close off all secondary entry points and focus your security personnel at the main gate.
- Have an alarm system in place that can be triggered by the guards in case there is a threat such as a mob gathering at the gate. This could be a formal alarm (sound and light) or a simple system where each guard carries a whistle.
- Train guards in crowd control as well as de-escalation techniques.
- Ensure that vehicles are safely parked inside; however, the vehicles must always be parked with the front facing outwards to ensure a rapid exit if required.
- Consider asking the community to assist with groups of community members to help monitor the facility.
- Specify rules of entry, such as a ‘no guns policy’.

## ✓ EMERGENCY CONTACTS

- Ensure that you have a list of emergency contacts immediately available including:
    - Police
    - Fire Brigade
    - Quick reaction force of the security company your organisation employs (where one is contracted)
    - Ambulance services
    - Community leaders
    - Religious leaders
    - Media
    - If you are working as part of a wider network, colleagues in other offices.
- Appoint a senior person to reach out to these emergency contacts as soon as a mob starts gathering.
- Especially community and religious leaders should be called to seek to calm down angry crowds.
- It helps to have a strong relationship built with these authorities prior to an incident to ensure that they respond quickly and appropriately in the event of an emergency.
- The process of actor mapping will be beneficial to identify who should be the priority points of contact and influence.

## ✓ ROCKS AND OTHER PROJECTILES

- Instruct guards to make rounds around and inside your compound and remove all rocks and other materials that could be used as projectiles.
- Consider putting blast film on the inside of the most exposed windows so that hurled projectiles do not result in flying fragments of shattered glass.

## COMPOUND ESCAPE

- Ensure that alternative escape routes are identified and are physically accessible to staff.
- All compound occupants must conduct evacuation drills on a quarterly basis.
- Pre-identify safe ‘MOVE TO AREAS’.

## LOCKDOWN

- Train staff in lockdown procedures as soon as they hear the alarm system.
- Do regular dry runs of lockdown procedures.
- Consider especially how to assist people with disabilities as well as other vulnerable people during a lockdown procedure.
- Designate buildings that are most secure in case of an attack.
- Appoint lockdown wardens for each building who have clear tasks to ensure that all people are safely inside, and doors are locked.
- Equip designated lockdown buildings with solid doors with bolt locks and/or metal grills.
- Always ensure that there is an escape route in case of fire.
- Instruct staff to take off all identification that identifies them as staff of the facility.
- Consider a well-stocked safe room with facilities for communication and other key essentials.

## PHYSICAL ATTACKS

- Ensure that first aid kits are available and strategically placed within the building.
- Staff must have basic first aid training and practice incident response.
- Buildings should be equipped with sufficiently large first aid kits able to deal with multiple victims, especially those that are designated as lockdown buildings.
- Ensure that your security guards have access to first aid materials and firefighting equipment.

## AFTER-CARE

- Ensure that you have psychological and medical care available to all those that have been affected.
- Provide special support for people who were specifically targeted
- Learn lessons together and debrief individuals as well as teams on what went well and what could be improved.
- Involve the community, including religious leaders, to understand the motivation behind any attack, condemn the attack, and invest in (renewed) acceptance-based security strategy efforts.

This document is published by **Insecurity Insight**. It is funded by the **H2H Fund**, which is supported by UK aid from the UK government.

Suggested citation: Citation: Insecurity Insight. 2020. Security Challenge: Mob attacks: Recommendations for protection of medical facilities against a mob attack. September 2020. Geneva, Switzerland: Insecurity Insight. Published September 2020.

Original publication developed by CBM with advisory provided by **RiskVisibility**. **CBM** is a Christian international development organisation, committed to improving the quality of life of people with disabilities in the poorest communities of the world irrespective of race, gender or religious belief. Contact CBM at: **hssunit@cbm.org**. CBM allows the use of this publication by other organisations upon explicit, written permission, provided that it is not altered or duplicated in a way that could mislead readers and it is not used for commercial purposes.

Disclaimer of liability: Neither Insecurity Insight nor CBM, Christoffel-Blindenmission Christian Blind Mission e.V. shall be held liable for any improper or incorrect use of the information described in this document and assumes no responsibility for anyone's use of the information.

Leading in disability inclusive development | cbm christian blind mission

Insecurity Insight

H2H Network Humanitarian Action Support

UKaid from the British people