Tool 3: Assessing threats, risks and vulnerability

A systematic approach to **assessing threats** includes working as a group with other programme workers to ask the following questions:

1. What are the facts surrounding the threat? (What do we actually know, not what we are assuming, about this threat?).
    - This is helpful because it reminds us to move away from gossip or conjecture. Sometimes a threat can be overblown or underestimated because of the way others perceive it. Try to only think about the facts.
2. Is there a series of threats that become more systematic or frequent over time? (Does a person make threats each day or do they just harass opportunistically? Are they escalating in terms of how close they are, such as finding individuals at their home or workplace?).
    - If something occurs multiple times, this increases the seriousness. It shows that making this threat is something the person/people feel a commitment too. Escalation of the threat—for example, someone was yelling at you when you were conducting outreach and now they have also found you online—is another sign that it is more serious.
3. Who is the person who is making the threats? (Is this someone known? Someone who has the ability to influence others? Someone who has information that could harm you or your colleagues?)
    - This question tries to understand how much power the person threatening has. For example, a police officer making threats is likely to be more dangerous than a stranger.
4. What is the objective of the threat? (Is it to change your behavior? Is it to scare? Is it a political tool to get votes?)
    - Thinking about this can help you decide whether the person may be willing to escalate. For example, if this is just to scare me then maybe the person isn't going to ever physically harm me, even if they say they will. Knowing this can also help you decide how to act.
5. How serious do you think the threat is? (Your own personal views on the topic)
    - Here is where you let your intuition and your understanding of the broader context inform your thinking on the threat's seriousness. This analysis can be conducted based on the threats or incidents recorded in the organisation's security log.

Practically speaking the organisation or programme can examine each threat or incident that is recorded in the Security Log (see Tool 1) and complete a table addressing each of the questions above.

Question	Answer
1. What are the facts surrounding the threat?	
2. Are the threats part of a series that has become more systematic or frequent over time?	
3. Who is the person/people making the threats?	
4. What is the objective of the threat?	
5. How serious do you think the threat is?	

A more detailed analysis of a threat can be done by looking more closely at the perpetrator or attacker. A perpetrator or attacker needs the following to be able to carry out a threat or an act of violence:

A. **Access**: to the potential victim or organisation, either physically or virtually. This could mean that they know where the programme is located and that they are able to enter unhindered; or that they can identify online workers through their online identities and use this to attack them or steal information.
B. **Resources**: anything that can be used to carry out the attack – for instance, information about the victim's location or weaknesses; having a weapon or transport or money that enables them to carry out an attack.
C. **Impunity**: this means that there are no consequences carrying out an attack: for instance no legal consequences or no social opposition to them doing so.
D. **Motive**: a reason for carrying out an attack or making a threat. This may be to do with their attitudes towards the programme or population, or their assumptions about the same. In some cases, we may wish to limit what others know about the type of work we do. In other cases, we may want them to better understand what we do because it benefits the broader society. In some other cases, we may decide that changing what others think is not our goal and we prefer to limit the other three domains.

The reason to look at these four factors is that it can also help to identify how each of them can be reduced or mitigated. There are no "right" answers, and often limiting something like access for an attacker could also limit it for your program beneficiaries (e.g., if you don't share your clinic's address online, neither an attacker nor person seeking HIV testing will find you easily). Making these decisions involves trade-offs. Once again, a table can be used to do this analysis in a systematic way.

	What does the attacker currently have?	How can your programme reduce these?	What are the trade-offs if you decide to act in this way?
A. Access			
B. Resources			
C. Impunity			
D. Motive			