



---

# **Strengthening the Security of HIV Service Implementers Working with Key Populations**

A virtual training for  
organizational leadership

---

April 2021





**Welcome,  
introductions, and  
background**



# Session Objective

- Welcome all participants and introduce participants to one another.
- Come to a shared understanding of training content and goals as well as participants' involvement in the training.
- Identify implementer security as an important and new area in HIV programming.



# Activity A. Introductions

- Name and title
- Experiences with security training
- One hope/expectation for this training

Group	Person 1	Person 2
A		
B		
C		
D		
E		
F		
G		
H		
I		



## Activity B. Group Norms

- These sessions will be recorded.
- Do not share identifying information about others when recounting security incidents.
- Participate fully.
- Come on time and remain for the entirety of each session.
- Do not share what you hear in this webinar beyond this space.



# Review agenda and expectations

To receive a certificate noting that you completed this training:

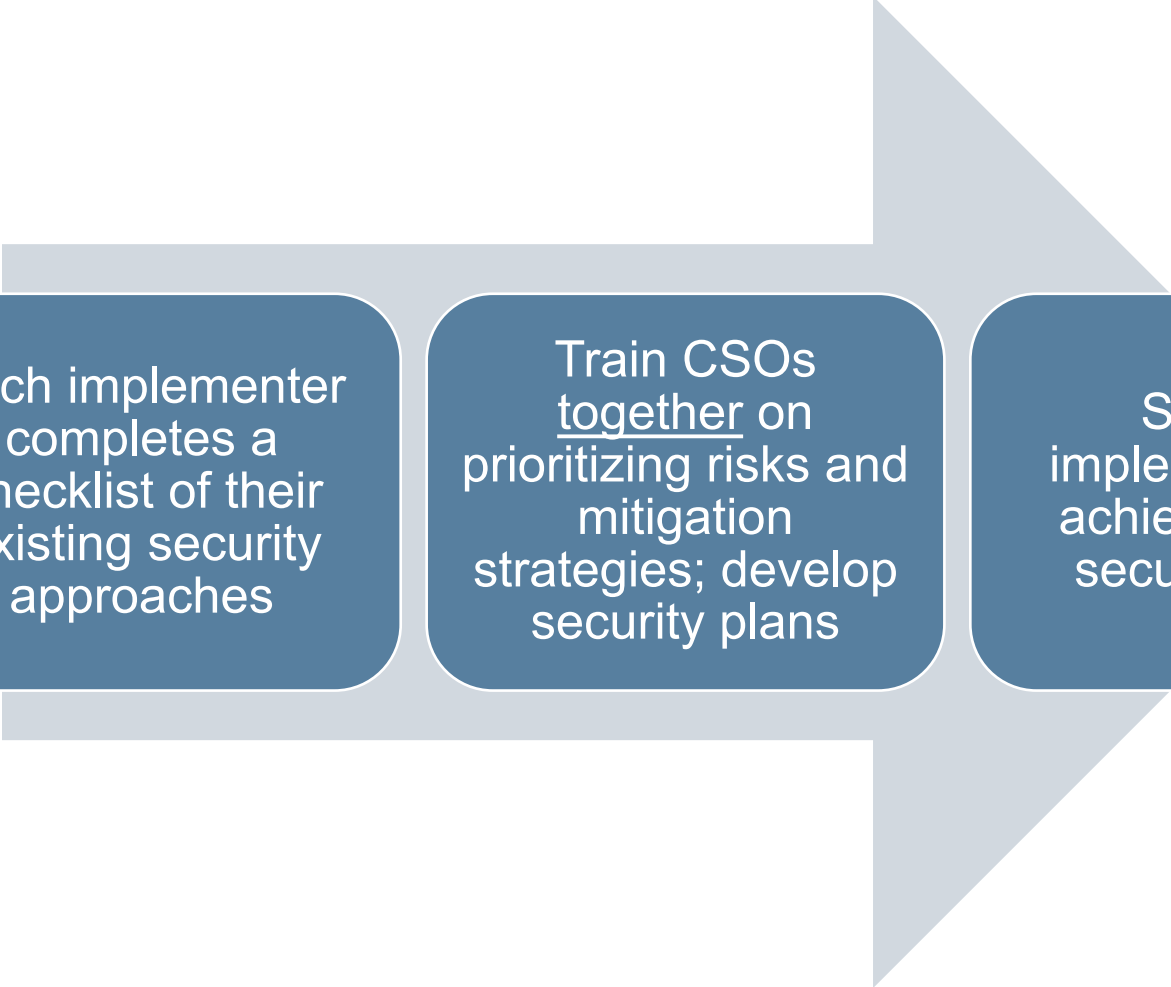
- Participants will participate in and contribute during each session (at least twice verbally and 5 times via chat per session).
- Participants will complete all homework assignments.
- Participants will complete the post-test and score at least 85%.

Training dates:

Time	Session
DAY 1	
8:00	Welcome, introductions, and background
8:45	Key terms and overarching recommendations
9:15	Threat identification and assessment
9:55	Day 1 closing
DAY 2	
8:00	Recap of Day 1 and HW #1
8:25	Limiting an aggressor's capacity to harm
9:00	Digital security
9:40	Review of our capacities and plan for skill sharing
9:55	Day 2 closing
DAY 3 - Special Session	
	Group presentations
DAY 4	
8:00	Day 2 recap and special session reflections
8:10	Using what you've learned: security challenge case studies
8:45	Risk assessment formula
9:05	Security planning
9:35	Next steps
9:50	Reflections and closing



# Process Overview



Each implementer  
completes a  
checklist of their  
existing security  
approaches

Train CSOs  
together on  
prioritizing risks and  
mitigation  
strategies; develop  
security plans

Support  
implementers to  
achieve priority  
security goals



# Step 1



- Cultivating and sensitizing external allies
- Influencing public perception of the project or organization
- Documenting harms for tracking and advocacy
- Protecting offices, drop-in centers, and other physical locations
- Keeping workers safe during physical and digital outreach
- Developing functional and institutionalized security protocols, including for emergencies
- Keeping data and communications safe
- Cross-cutting: emergency preparedness, digital safety, COVID-19





## Step 2



### Workshop Objectives

- Identify security strengths and gaps and share strengths among implementers
- Prioritize security risks faced by the program and determine the most important gaps for each CSO to address
- Draft CSO-specific security plans that address priority risks and how skills will be built to manage that risk

# Step 3

Each implementer completes a checklist of their existing security approaches

Train CSOs together on prioritizing risks and mitigation strategies; develop security plans

Support implementers to achieve priority security goals

Risk (of something): **A break-in at the clinic with client records stolen**

Threats	Vulnerabilities	Existing capacity	Required capacity
<b>High</b> <ul style="list-style-type: none"><li>• Outreach workers have been followed back to clinic by yelling groups who say we promote homosexuality</li><li>• Threatening messages graffitied onto clinic</li></ul>	<ul style="list-style-type: none"><li>• We are in a neighborhood with little street traffic in the evenings</li><li>• We do not have any security guards at the clinic after 5 pm</li><li>• We don't have a way to monitor visitors during the day</li><li>• Staff do not always lock up patient charts</li><li>• Windows and doors do not have bars; can be broken with rocks</li></ul>	<ul style="list-style-type: none"><li>• We have a security guard while the clinic is in operation (9 am–5 pm)</li><li>• We have the USAID and MOH logo on our sign</li><li>• We have introduced ourselves and explained our work to senior law enforcement officers working in the district</li><li>• We have locked cabinets to store all paper client records</li><li>• We use UICs and keep mostly encrypted electronic information</li></ul>	<ul style="list-style-type: none"><li>• Visitor monitoring logs</li><li>• Retraining for all staff on safe document storage (clean desk policy)</li><li>• Talk to landlord about the nature of our work</li><li>• Install physical security measures for windows and doors</li><li>• Create log for security challenges to track trends; consider using it to advocate with donor for funds for increased security presence</li></ul>

# Implementer security in HIV programs: An incomplete history

- Longer history of violence/crisis response for beneficiaries of KP HIV programs (e.g., Avahan, early 2000s) and LGBT-led rights-focused organizations (e.g., Dignity for All consortium, 2012)
- KP programs saw and increasingly documented implementer insecurity
  - Arrests and detentions
  - Offices raided/broken into
  - Attacks on personnel (physical, sexual, economic, and emotional)
- LINKAGES and Frontline AIDS develop a toolkit; LINKAGES with Synergia develop training materials focused on KP HIV program implementers (2018)
  - Efforts to improve data safety specifically (2019)
- LINKAGES/EpiC extend security work across the project, into digital security and index testing, and into new regions (MENA, 2019-21)



## Violence Targeting LGBT CBOs & Services

### Belarus

Following an unsuccessful attempt to register an LGBT-focused CBO in January 2013, LGBT activist Ihar Taikharuk was "questioned, beaten, and subjected to threats of abuse for being gay by the Belarusian police."<sup>102</sup> Following the attempted registration, members of the LGBT community reported that police summoned them and physically assaulted at least one individual.<sup>103</sup>

### Côte d'Ivoire

Alternatives Côte d'Ivoire, which



## Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations

MARCH 2018

## Ensuring compliance with the LINKAGES Data safety and security checklist

This resource is made possible by the generous support of the American people through the U.S. Agency for International Development (USAID) and the U.S. President's Emergency Plan for AIDS Relief (PEPFAR) through the terms of cooperative agreement AID-COA-16-0005, and additional support from LINKAGES, funded by the Department of Health and Human Services, Office of the Assistant Secretary for International, Policy, and Programs.



Security Protections for Organizations  
Working with Key Populations to  
Strengthen HIV Programming  
in the Middle East and North Africa

## AMAN MENA

Secure in the MENA region

December 2020





# What, Who, Why?

In your context:

- What do security incidents affecting implementers look like?
- Who perpetrates abuse against KP program implementers?
- Why do attacks on implementers occur?

## **KP program implementers can include:**

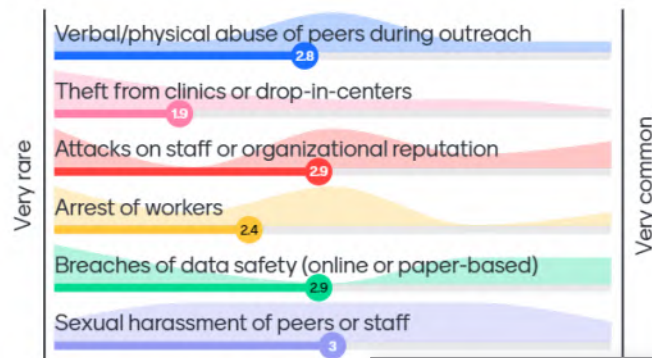
- Outreach workers/community mobilizers
- Peer educators/navigators
- Community health workers
- Community members
- Program directors and managers
- Program officers
- Drop-in center workers
- Clinicians (e.g., doctors, nurses)
- Counselors and psychosocial support providers
- Office staff (e.g., receptionists)
- Support staff (e.g., drivers, guards)
- Community activists, advocates, and campaigners
- Lawyers and paralegals
- Allies and champions



# Activity C. What, Who, Why?

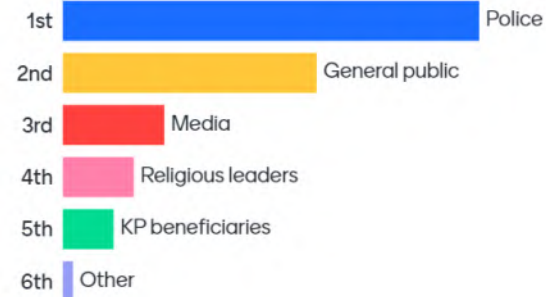
Go to [www.menti.com](https://www.menti.com) and use the code 98 42 23 8

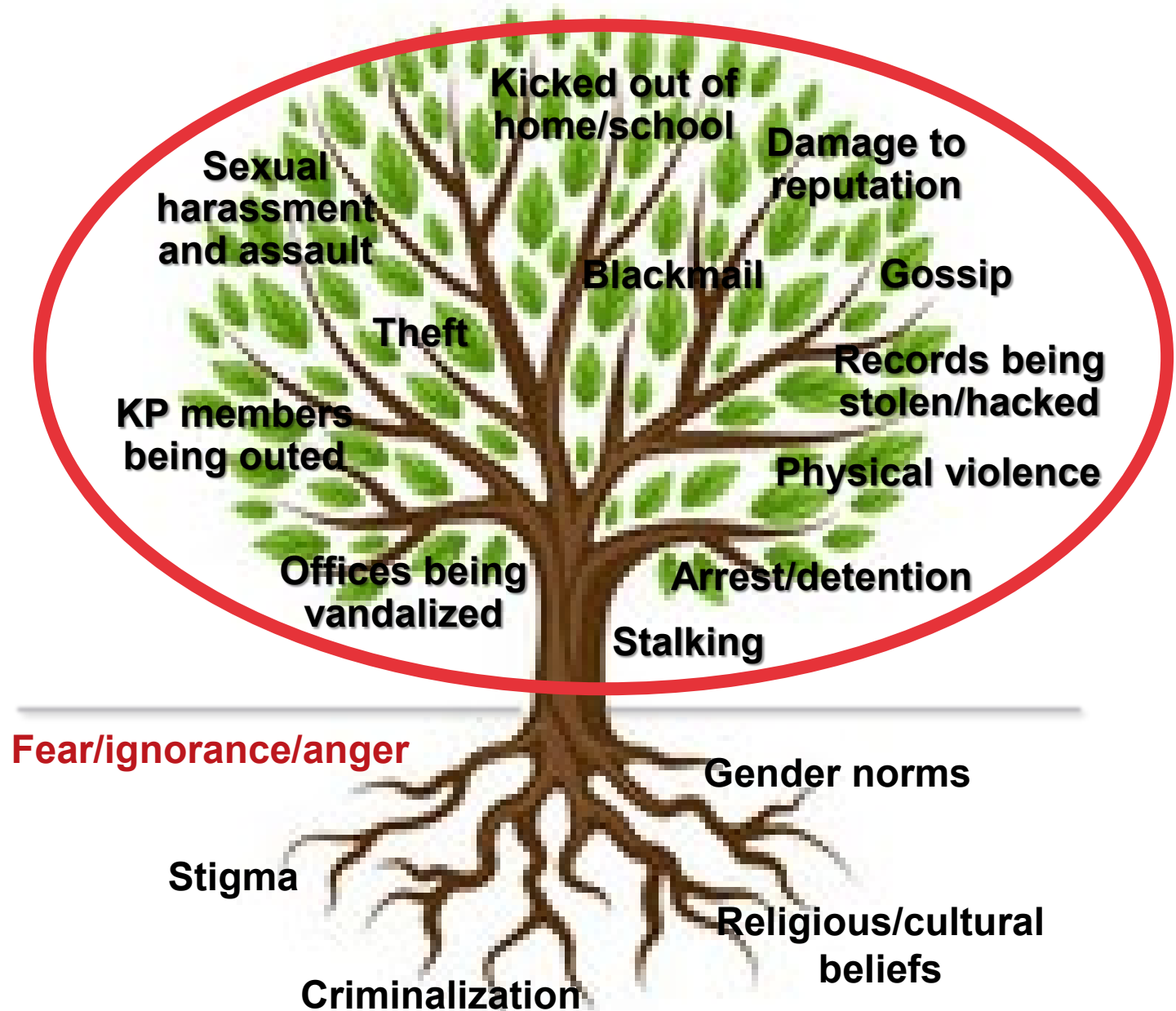
Thinking of your KP program, how common is each of these security incidents?



The code lets your audience join the presentation. It expires in 2 days.

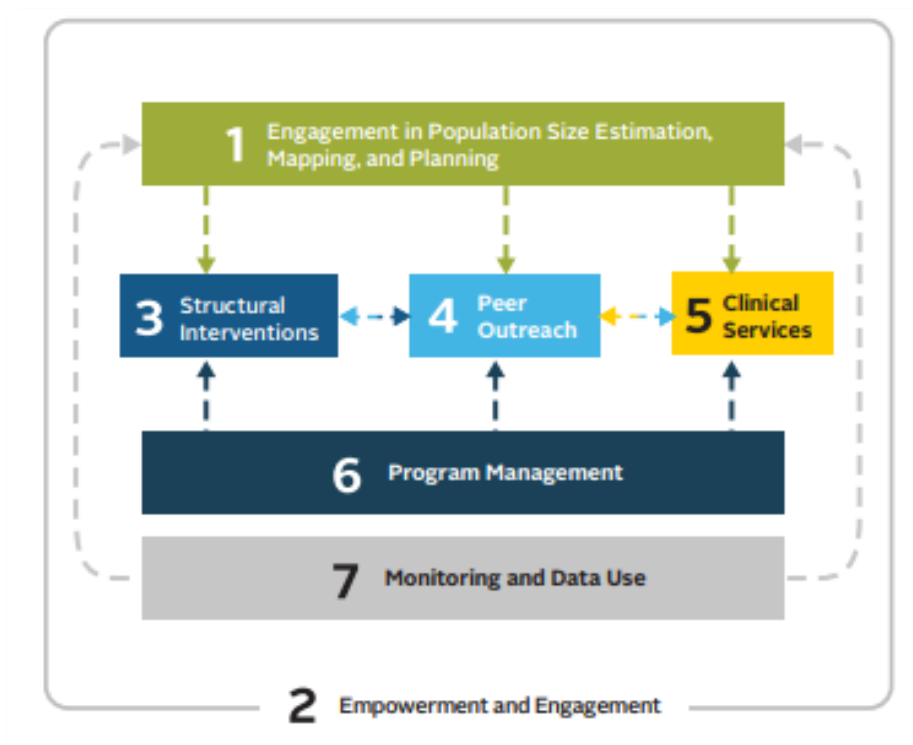
Who perpetrates violence against KP program implementers?





# How do security challenges affect KP programs?

## Seven areas of key population programs<sup>1</sup>



1. It can be difficult to undertake behavioral or biomedical surveys limiting reliable data.
2. Hiring members of KPs or engaging civil society organizations (CSOs) led by KP members is more difficult.
3. Need for intensive stigma-reduction trainings for HCWs, especially if working with KP members brings secondary stigma and abuse.
4. Harassment limits outreach.
5. Clinical staff burnout increases.
6. Shifts in management focus make it difficult to meet programmatic objectives.
7. If data cannot be kept safe, what can be collected is severely limited.



# **Key terms and overarching recommendations**





# Session Objective

Define “security,” “risk,” “threat,” “capacity,” and “vulnerability,” and discuss the key recommendations for security of implementers in KP programs.



## Activity D. Definition: Security

What does “security” mean?

- A. Being sure that you are completely safe.
- B. Being free from intentional violence.
- C. Having a first-aid kit.

While the word “security” is sometimes used interchangeably with safety, security is focused on freedom from intentional harm. Safety includes freedom from harms such as sickness and natural disasters, which won’t be touched on in this training.



## Activity D. Definition: Risk

What does “risk” mean?

- A. The probability that something harmful will happen.
- B. Being careful.
- C. Planning ahead to avoid danger.

While the word “risk” can refer to both the possibility of harm and someone/something that creates a hazard, in this training we will talk about risk as the probability that something harmful will happen.



## Activity D. Definition: Threat

What does “threat” mean?

- A. An indication/sign that someone wants to hurt, damage, or punish us.
- B. A supportive statement.
- C. A bad omen.

Threats can be verbal, such as, “I will hurt you.” However, threats can also be actions. In this training, we will talk about threats as coming from outside of ourselves (i.e., we will not cover ideas such as self-harm).



## Activity D. Definition: Capacity

What does “capacity” mean?

- A. A sign that someone wants to hurt, damage, or punish us.
- B. Any resource (financial, ability, contacts, infrastructure, personality, etc.) that we can use to improve our security.
- C. How dangerous something is.

Capacities can be almost anything. A great sense of humor can help defuse a tense situation. Being connected to someone in the national AIDS program might keep others from bothering you. A car with strong locks can protect against theft.



## Activity D. Definition: Vulnerability

What does “vulnerability” mean?

- A. Anything that increases our exposure to those who want to hurt us.
- B. Anything we do to keep ourselves safe.
- C. A sign that someone wants to hurt us.

Our goal is not to make ourselves completely invulnerable. To be alive is to be vulnerable. However, we can identify our vulnerabilities and determine whether some of them can be reduced.

# Vulnerability is a tricky concept

- A “vulnerability” is not the same thing as a “weakness.”
- A capacity in one context can be a vulnerability in the next context.
- Some capacities/ vulnerabilities cannot be changed.
- The goal is to be aware of your vulnerabilities and capacities and act in a way that takes these into account, with ***each person deciding what is right for them.***





# Activity E. Homework: Overarching recommendations

- A 1. Make HIV program principles and approaches the foundation of security efforts.
- B 2. Make security a priority and resource it explicitly.
- C 3. Make a safe workplace the employer's responsibility.
- D 4. Plan ahead and make sure that everyone knows the plan (while maintaining flexibility).
- E 5. Explicitly discuss the level of risk that is acceptable organizationally and individually.
- F 6. Operate with a knowledge of both the actual risks and their underlying causes (including legal frameworks).
- G 7. Acknowledge the different vulnerabilities and capacities of each worker in security planning.
- H 8. Get to know all stakeholders, not just obvious allies.
- I 9. Identify both threats (physical, digital, psychological) and security strategies holistically.
- J 10. Be together, work in coalition, and learn from one another.

## Homework #1: Recommendation reflections

- Following this session, each group will be assigned to one recommendation.
- Read more about your recommendation in the training cheat sheet.
- Be prepared, next session to (1) describe this recommendation, (2) share how your program is already using this recommendation, and (3) how it could use this recommendation.





# Threat identification and assessment



# Session Objective

Identify threats and determine their seriousness.



# Threat types

- **Direct threat** – An indication that someone wants to inflict pain or damage me/my organization specifically.
- **Indirect threat** – An indication that someone wants to inflict pain or damage a broader group of people that I am a part of, but not me/my organization specifically.
- **Security incident** – Situations where harm occurs, but we're unsure if the incident is a threat or more of a coincidence.



# Activity F. Label Each Threat

Incident	Type of threat to <u>you</u> (direct threat, indirect threat, security incident)
<b>A.</b> You are the director of CSO 1, an organization that provides HIV services to MSM. An influential local leader accuses CSO 2 of promoting homosexuality. CSO 2 offers the same services to MSM that your organization does. Someone breaks the windows of CSO 2 and puts graffiti on the home of CSO 2's director.	<b>Indirect threat:</b> It's not a threat directly to you but it does target a group that you are part of (people providing HIV services to MSM)
<b>B.</b> You are a peer outreach worker who distributes condoms. A police officer stops you and tells you that if he sees you again, he will have you arrested.	<b>Direct threat:</b> This threat is about you and directed toward you
<b>C.</b> You are a nurse. An index client gives you the name and address of her sexual partner. When you visit the home of the named partner, he refuses to speak to you. Later that day, you receive three calls from an unknown number. The caller never says anything, but always breathes heavily into the phone.	<b>Security incident:</b> You don't know who is calling and if you're being targeted for any specific reason.



# Recording Threats

Being able to catalogue all three threats is important and can help you provide documentation, including to the donor, and track patterns

- Riskier locations or activities
- Common perpetrators
- Whether an indirect threat to larger group
- Whether violence is intensifying
- Who is most at risk





# Security Log

Security Incident Log			
	Question	How to Answer	Response
1	Security incident number	Begin with number 1 and continue; the numbering allows security incidents to be linked to one another (see question #14)	
2	Date of incident	Type as YEAR-MONTH-DAY (e.g., 2019-02-17 for February 17, 2019) in order to organize this security event log by date	
3	Time of incident	Specific time of day (if known), or more general (morning, afternoon, evening, night)	
4	Perpetrator	If known and safe to list, or use a more general term such as "law enforcement officer"	
5	Affected organization	Name of HIV program implementing partner (i.e., community-based organization's name)	
6	Target	Specific person or type of staff, physical space (e.g., name of a specific hot spot), website, database, etc. Do not name individuals here unless you have their permission to do so.	
7	Where incident occurred	Physical address, online, by phone, etc.	



# Assessing threats: How serious is it, really?

1. What are the facts surrounding the threat?
2. Is the threat part of a series that has become more systematic or frequent over time?
3. Who is the person who is making the threats?
4. What is the objective of the threat?
5. Do you think the threat is serious?



# Example

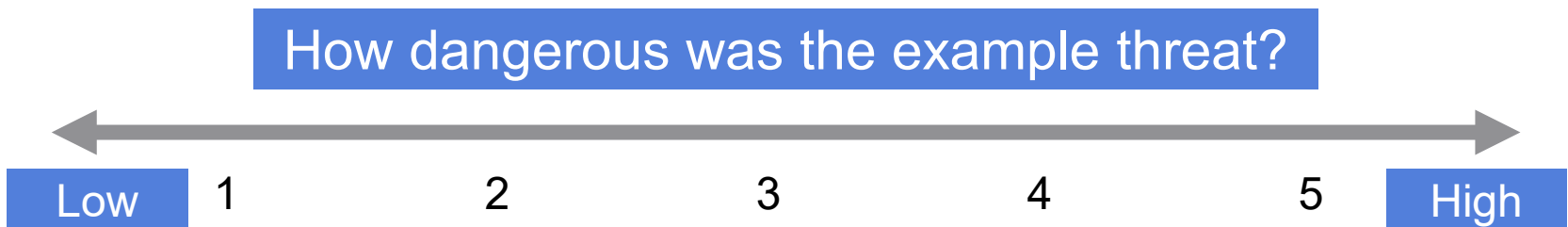
Question	Answer
What are the facts surrounding the threat?	A group followed two peer educators to three different hot spots. The group yelled at the educators and said they promoting immorality.
Are the threats part of a series that has become more systematic or frequent over time?	Yes, this is the third time that these peers have been targeted with verbal abuse. The first time occurred a month ago and happened at just one hot spot. Now they are following peers between hot spots.
Who is the person/people making the threats?	They seem to be local community members who live near the hot spot. Several of them are known to be members of a church that preaches constantly against homosexuality.
What is the objective of the threat?	To prevent outreach and to follow the teaching of their minister.
Do you think the threat is serious?	Somewhat. Our peer educators' mental health is being impacted, which is a big concern. We do not believe the group will become physically violent.





# Activity G. Assessing Threats Based on Impact

- After you decide how serious a threat is (i.e., how likely it is to occur), don't forget to consider the impact of the threat when assessing its potential to cause harm.
- For example, a threat that could cause your organization to be shut down is more dangerous than one that could cause disruption to a few days of services.
- In your opinion, how dangerous was the example threat? (type your answer in the chat)

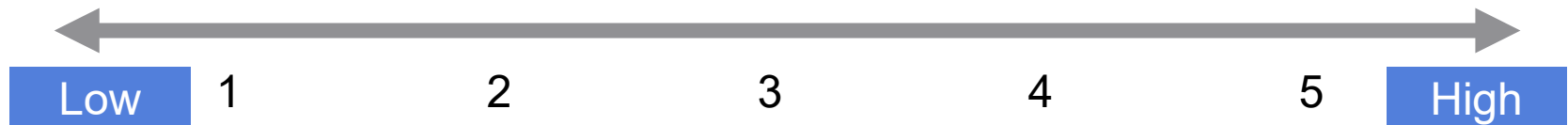




# Activity H. Considering Our Own Threats

Question	Answer
What are the facts surrounding the threat?	
Are the threats part of a series that has become more systematic or frequent over time?	
Who is the person/people making the threats?	
What is the objective of the threat?	
Do you think the threat is serious?	

How dangerous was the example threat?





**Day 1 closing**



# Session Objectives

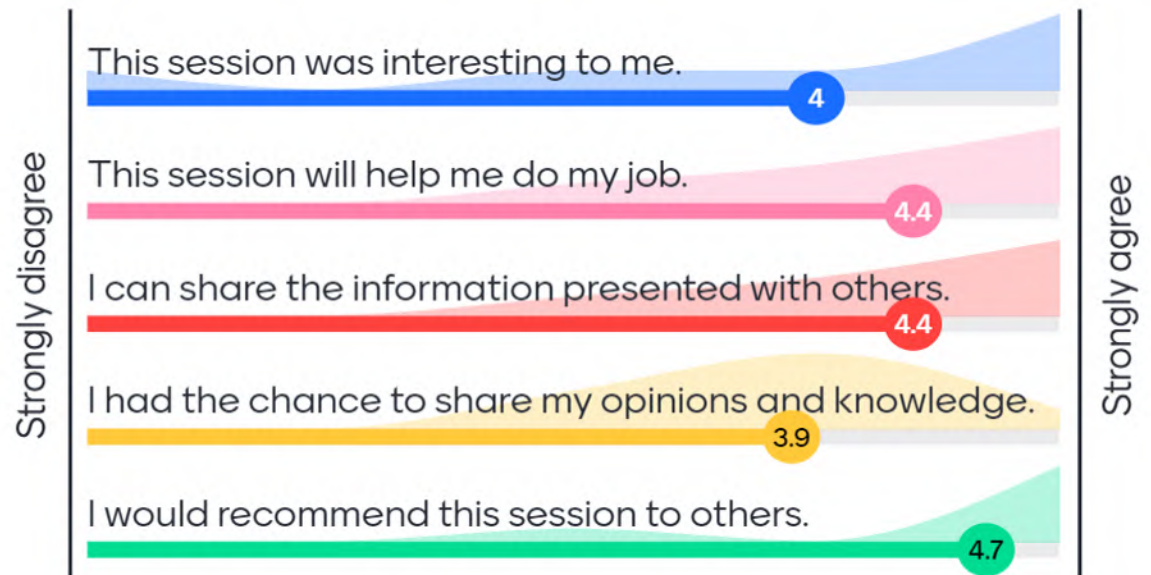
Evaluate the day.



# Activity I. Menti, Day 1 closing

Go to [www.menti.com](https://www.menti.com) and use the code 88 64 96 0

Please share your opinions about today's session.





---

# Strengthening the Security of HIV Service Implementers Working with Key Populations

A virtual training for  
organizational leadership

---

April 2021

## DAY 2





# Recap of Day 1 and Homework #1



# Session Objectives

- Share homework #1 answers.
- Remember the topics covered on Day 1.





# Activity J. Recommendation Reflections

1. Make HIV program principles and approaches the foundation of security efforts.
2. Make security a priority and resource it explicitly.
3. Make a safe workplace the employer's responsibility.
4. Plan ahead and make sure that everyone knows the plan (while maintaining flexibility).
5. Explicitly discuss the level of risk that is acceptable organizationally and individually.
6. Operate with a knowledge of both the actual risks and their underlying causes (including legal frameworks).
7. Acknowledge the different vulnerabilities and capacities of each worker in security planning.
8. Get to know all stakeholders, not just obvious allies.
9. Identify both threats (physical, digital, psychological) and security strategies holistically.
10. Be together, work in coalition, and learn from one another.

## Homework #1

Describe: (1) the recommendation, (2) how your program is already using this recommendation, AND (3) how the program could use this recommendation.

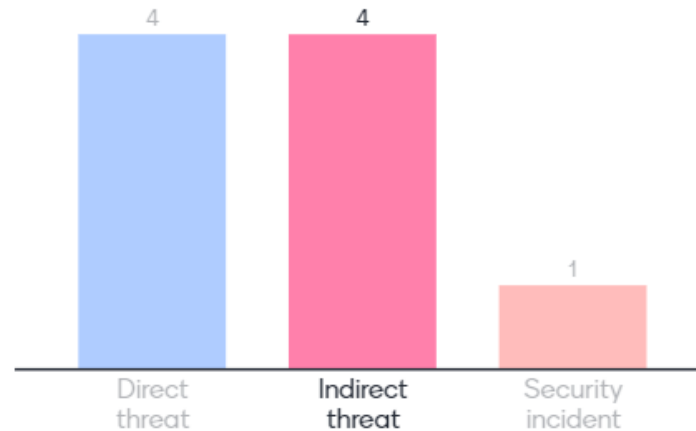


# Activity K. Menti Day 1 Recap

Go to [www.menti.com](https://www.menti.com) and use the code 38 86 45 9

You are a peer educator. You learn that two other peer educators in your province were arrested during outreach. What kind of threat is this, to you?

 Mentimeter



Press ENTER to hide correct

9





# Limiting an aggressor's capacity to harm



# Session Objective

Describe what can be done, and by whom, to limit an aggressor's ability to cause harm.



# Activity L. What Does a Potential Attacker Need?

An attacker needs:

- **Access:** to the victim physically or virtually
- **Resources:** anything that can be used to carry out the attack – information on the victim's location or weaknesses; weapon; transport; money; etc.
- **Impunity:** legal and/or social
- **Motive:** reason to act

Type in the chat: what does an attacker need to be able to carry out an attack (in a physical or virtual space)?



# Activity M. Scenario 1, Outreach

Marvin is an outreach worker (ORW) for an organization that delivers condoms and lubricants. He travels alone to places, such as night clubs, where gay men socialize. While there, he provides three condoms and three lubricants to each person (in pre-packaged bags per organizational policy). Several weeks in a row, different men at one specific bar have aggressively demanded more condoms. Each time, Marvin refused, explaining the CSO policy. One night, a man who had yelled at Marvin several times throws a full beer bottle at him, striking him hard on the head.

**What could be done to limit access, resources, motive, and impunity to prevent this situation from occurring again?**



# Scenario 1 possible answers

- Marvin's organization could:
  - Change their policy re: condom distribution (motive)
  - Send out peers in groups of two or more (access/impunity)
  - Stop providing services to this hot spot OR only provide services if hot spot owners offer better protection to outreach staff OR leave condoms/lubricants in a bathroom or other location (access/impunity)
  - Engage a local champion at the hot spot who can distribute the condoms or explain the policy (access/motive)
- Marvin could:
  - Report the incidents to his organization so they can respond (all)
  - Meet people outside before they enter the bar (resources)



## Activity M. Scenario 2, Clinic

Crystal is a nurse with a CSO-supported clinic. She provides sexual and reproductive health services to sex workers. She has helped several sex workers access counseling to deal with violent relationships. One morning, an unknown man comes to the clinic and asks for Crystal. The receptionist allows him in. He finds Crystal and threatens her with a knife, saying she better, “stay out of my personal life.” Crystal finds out later that the unknown man is the abusive boyfriend of one of the sex workers who Crystal had helped.

**What could be done to limit access, resources, motive, and impunity to prevent this situation from occurring again?**





# Scenario 2 possible answers

- Crystal's organization could:
  - Develop and implement an admittance policy that includes
    - Writing down each visitor's name and reason for a visit (impunity/access)
    - Calling back to the relevant staff to ask if the visitor is expected before they are admitted (access)
    - Having well-marked public areas where staff come and meet visitors who are not clients (access/impunity)
    - Checking each visitor for weapons (resources)
  - Remind all staff to talk to clients about circumstances under which it may be better not to share information with a violent partner (motive)
- Crystal could:
  - Remind her clients that it may not be appropriate to share the nature of the support they receive at the clinic with violent partners (motive)
  - Remind her clients not to take home any documents about violence that their partner may see and react negatively to (motive)



## Activity M. Scenario 3, Going online to off-line

An online ORW, Patrick, meets new potential service users on Grindr and encourages them to get tested. The men he meets on Grindr often want to meet him off site before they are willing to go to a clinical facility. Several times, when Patrick met potential service users in person, they wanted to have sex with him. One man, Andrew, was incredibly insistent. After Patrick said he did not wish to have sex, Andrew came to the CSO's office looking for Patrick on multiple occasions and even showed up at Patrick's other job (waiting tables at a restaurant) after finding information about Patrick online.

**What could be done to limit access, resources, motive, and impunity to prevent this situation from occurring again?**



# Scenario 3 possible answers

- Patrick's organization could:
  - Have clear policies and training regarding the information that each online ORW can share; e.g., no photos, no last names, no personal information (access, resources)
  - Have clear policies stating that ORWs cannot have relationships with clients; the policies could be accompanied with scripts for the ORWs to use if clients ask them to be involved in a relationship (motive)
  - Have a policy that states that online ORWs should never meet off site with clients being transitioned from online to off-line or that a new ORW must be the person to handle the transition (access)
  - Have a policy on how to protect staff who may be at risk, including funds for relocation (access)
- Patrick could:
  - Limit information available about himself online (e.g., not create a LinkedIn profile that includes your organization, full name, and photo)
  - Report concerning clients to the organization immediately and seek guidance



## Activity M. Scenario 4, Index testing

An index client shares the names of three sexual partners. Mary, a health care worker, successfully links named partners #1 and #3 to services but cannot reach partner #2 by phone. Mary tries to find partner #2 at home. She uses public transport, as per program policy. When Mary tells partner #2 why she has come, partner #2 threatens Mary with a pot of boiling water. Mary leaves immediately. While Mary must wait for public transport to return to the office, she is extremely frightened.

**What could be done to limit access, resources, motive, and impunity to prevent this situation from occurring again?**



# Scenario 4 possible answers

- Mary's organization could:
  - Make sure all index clients are screened for intimate partner violence (IPV) so ORWs do not go to the homes of violent clients (access)
  - Have policies that dictate no client home visits without permission/voluntarism (access)
  - Have policies that allow for private transport during community visits or in special circumstances (access)
  - Have clear guidelines for index testing that dictate which modalities are appropriate in different circumstances (access, motive)
  - Have policies that dictate no one does outreach alone (access/impunity)
- Mary could:
  - Suggest that an outreach event occur in partner #2's community; several people can be invited to attend, including partner #2 (motive)



# Activity N. What do these solutions have in common?

In each scenario, the solutions are primarily the responsibility of the organization and not the individual.

Organizations acknowledge their responsibility to their workers' safety. They do not simply rely on staff/volunteers' best judgment.

## Scenario 1 possible answers

- Marvin's organization could:
  - Change their policy re: condom distribution (motive)
  - Send out peers in groups of two or more (access/impunity)
  - Stop providing services to this hot spot OR only provide services if hot spot owners offer better protection to outreach staff OR leave condoms/lubricants in a bathroom or other location (access/impunity)
  - Engage a local champion at the hot spot who can distribute the condoms or explain the policy (access/motive)
- Marvin could:
  - Report the incidents to his organization so they can respond (all)
  - Meet people outside before they enter the bar (resources)

## Scenario 2 possible answers

- Crystal's organization could:
  - Develop and implement an admittance policy that includes
    - Writing down each visitor's name and reason for a visit (impunity/access),
    - Calling back to the relevant staff to ask if the visitor is expected before they are admitted (access),
    - Having well-marked public areas where staff come and meet visitors who are not clients (access/impunity)
    - Checking each visitor for weapons (resources)
  - Remind all staff to talk to clients about circumstances under which it may be better not to share information with a violent partner (motive)
- Crystal could:
  - Remind her clients that it may not be appropriate to share the nature of the support they receive at the clinic with violent partners (motive)
  - Remind her clients not to take home any documents about violence that their partner may see and react negatively to (motive)

## Scenario 3 possible answers

- Patrick's organization could:
  - Have clear policies and training regarding the information that each online ORW can share; e.g., no photos, no last names, no personal information (access, resources)
  - Have clear policies stating that ORWs cannot have relationships with clients; the policies could be accompanied with scripts for the ORWs to use if clients ask them to be involved in a relationship (motive)
  - Have a policy that states that online ORWs should never meet off site with clients being transitioned from online to off-line or that a new ORW must be the person to handle the transition (access)
  - Have a policy on how to protect staff who may be at risk, including funds for relocation (access)
- Patrick could:
  - Limit information available about himself online (e.g., not create a LinkedIn profile that includes your organization, full name, and photo)
  - Report concerning clients to the organization immediately and seek guidance

## Scenario 4 possible answers

- Mary's organization could:
  - Make sure all index clients are screened for intimate partner violence (IPV) so ORWs do not go to the homes of violent clients (access)
  - Have policies that dictate no client home visits without permission/voluntarism (access)
  - Have policies that allow for private transport during community visits or in special circumstances (access)
  - Have clear guidelines for index testing that dictate which modalities are appropriate in different circumstances (access, motive)
  - Have policies that dictate no one does outreach alone (access/impunity)
- Mary could:
  - Suggest that an outreach event occur in partner #2's community; several people can be invited to attend, including partner #2 (motive)



# Digital security



# Session Objective

Describe the vulnerabilities inherent to digital platforms and identify risk-reduction strategies within each.





## Activity O.

**Menti: What devices are you using and what do they say about you?**

- What devices do you use in your daily life?
- What could someone learn about you if they had access to your phone/tablet/computer?



# Use passwords and make them strong

- Have more than one.
- Change your passwords on a regular basis (Tip: reset your passwords, then set a reminder on your phone three months from that day to change them, repeat).
- A strong password has about 10 characters or more; ideally including: upper case letters, lower case letters, numbers, and symbols.



# Use two-step verification

- Email, social media, and other sites allow you to turn on two-step verification, which asks for a code from an app or texts you a number to enter when you or someone else tries to log in to your account from an unfamiliar browser or computer.
- It's a small annoyance for you, but a huge annoyance to someone who is trying to break into your account.
- <https://iheartmob.org/resources/tech>



Technical Safety Guide



# KeePass

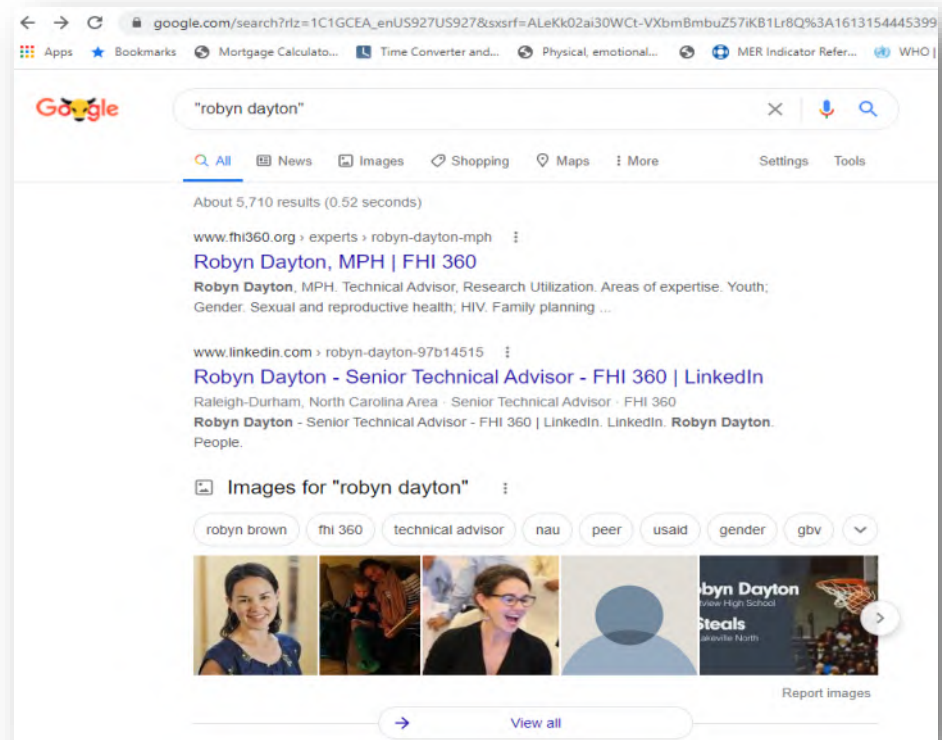
- Free, open source, password manager
- Keeps passwords safe
- You only have to remember one single master key to unlock the whole database of your passwords
- <https://keepass.info/>



**KeePass**  
Password Safe

# Search for yourself

- Everything from our name and email address to our home address and bank information is online.
- Once you find information about yourself online, go about getting it removed.



# Limit what you share about yourself

- Do not mention details about where you live or where you like to hang out
- Don't tag a location that you're in or post pictures that allow people to identify your location
- Watch out for automatic sharing of location on social media (GPS-enabled devices)

Where are these people?

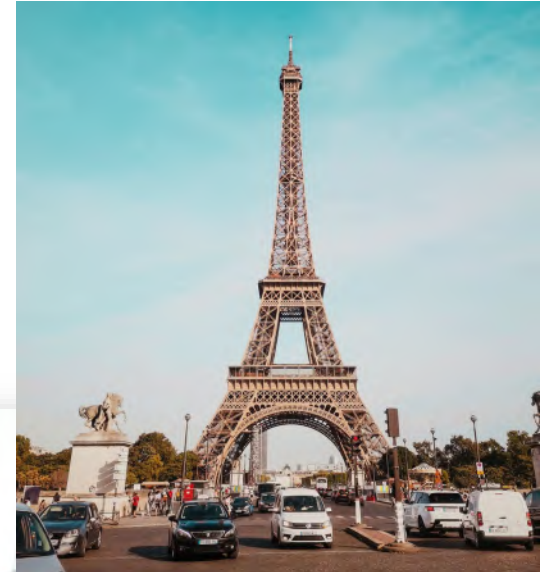


Photo credit: Tomas Nozina

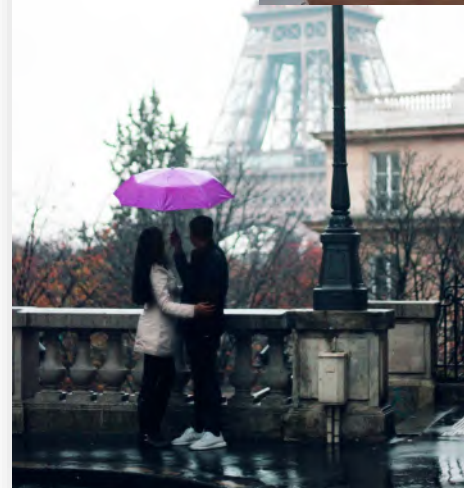


Photo credit: Loly Galina

# Limit what you share about yourself (cont.)



- Avoid sharing information that will allow others to know your daily schedule.
- Be careful about posting information that can be used to figure out your security question answers:
  - name of a childhood pet
  - your full birth date
- <https://safequeers.org/> has more on safe use of dating websites, etc.

# When information is used against us

- Doxxing occurs when people search for and publish private or identifying information on the internet about someone else that they wish to harm.
- It is a tactic used to make individuals feel unsafe.
- Doxxing is easier than ever because much of our information is online.



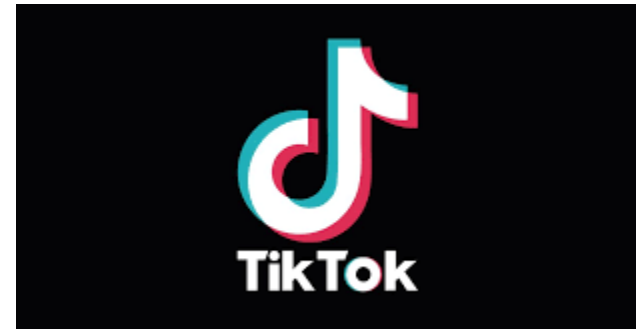




## Activity P. What are we sharing on social media?



- What social media do you use?
- What could someone learn about you there?



# Question Q. What could someone learn about me from these social media posts?





## Limit what you share about others

- Photos and videos quickly reveal identities, locations, and personal information.
- Get consent before taking and posting photos.
- Cameras will embed hidden data. Photo sharing sites may include this content when you upload the photo. Be careful!
- If no photographs are allowed in certain spaces, share this information widely.



# If you are harassed online, you can act

- **Ignore/block them** – engaging can become overwhelming
- **Report them** – and ask your friends to report them! Use [Social Media Safety Guides](#) to see more on how to report on Facebook, Instagram, etc.
- **Expose them** – you can take photos of the harassment and hold them accountable by sharing proof of their harassment
- **Engage them** – by explaining the stance that you took
- **Seek support** – it can be traumatizing; speak to someone supportive
- **Go anonymous** – e.g., attach a

## Activity R.

Have you used any of these methods? What was the result?



Social Media Safety Guides

Staying safe on social media- We've got your back!

Introducing our new Social Media Safety Guides for Facebook, Twitter, Reddit, Tumblr, and Youtube! We have worked hard alongside each of these platforms to make it easier for you to stay safer online. Every guide gives user-friendly information on how use different platforms' reporting and privacy tools – and for the very first time all of this information is gathered in one location.



Twitter



Facebook



Instagram



Tumblr



Reddit



Youtube



# Texting options

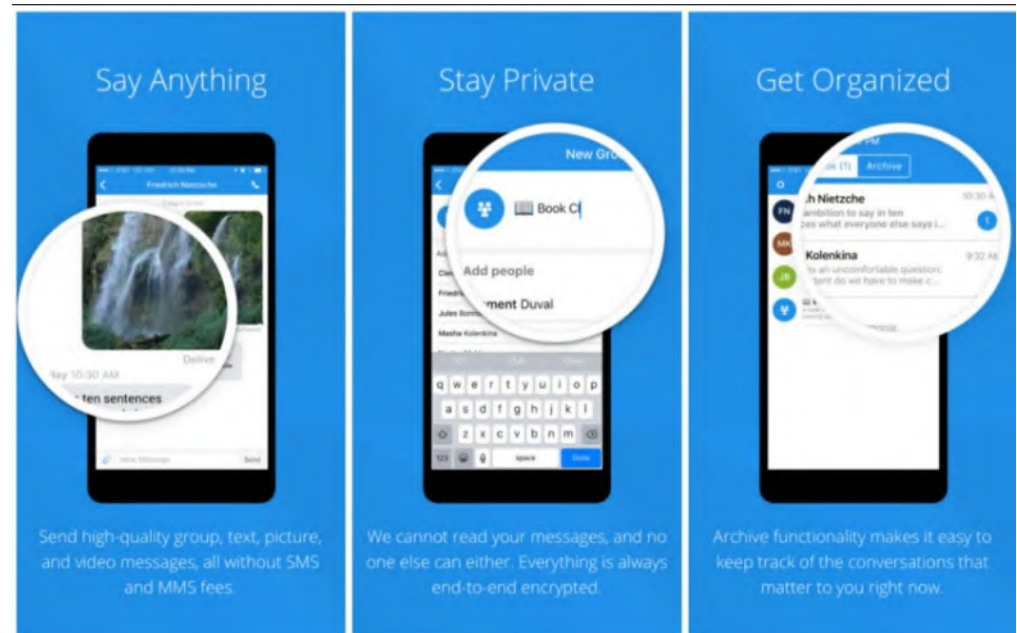
- WhatsApp is a popular communication option (2 billion monthly users) owned by Facebook
- Communication is encrypted end-to-end, but BIG security gaps remain:
  - Anyone with your phone number can see: your “about” blurb and photo, when you were last online, and whether you’ve read a message (check privacy settings to change).
  - Facebook can access: who you contact, when, how often, and from where (this cannot be turned off).
  - Police with a warrant can ask Facebook for: who you’ve called or texted, or who has called and texted you.
  - If you choose to back up your WhatsApp data to iCloud or Google Drive, messages are not encrypted there.





# If not WhatsApp, what else?

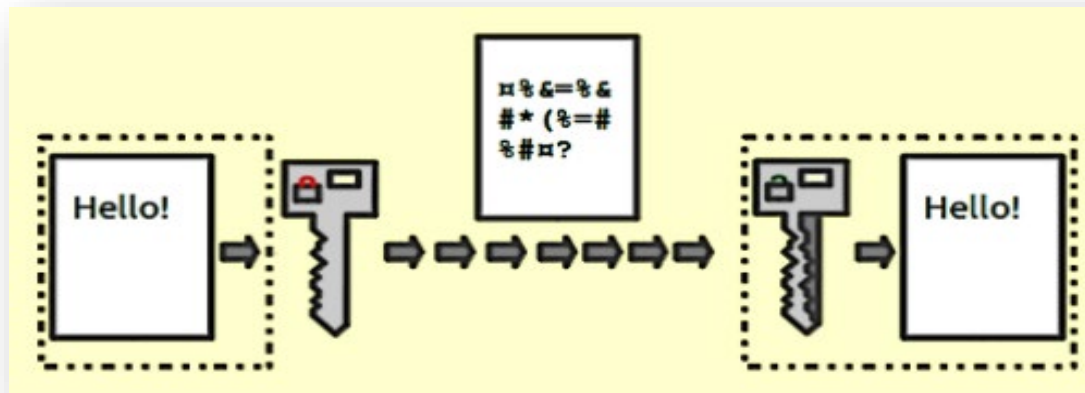
- Signal (free app) is more secure; encrypted end-to-end
- Can have group audio calls
- You can send out messages that will disappear after a set time



# Encryption and document protection

- Consider encryption (Veracrypt lets you create a secret folder not visible unless you know how to look for it)
- Consider changing file names on your computer
  - Instead of “MSM outreach\_X location”
  - Use “Project activities\_Code name for X location”

## What is encryption?





# Activity S. Linking Problems to Solutions

Problem	Answer	Solution options
1. Online outreach workers are receiving unwanted sexual advances	A, B, C, D, E	A. Include guidance on what online workers can share, including names/photos/locations
2. Online outreach workers are being stalked by clients	A, B, C, D, E	B. Provide scripts to guide online conversations and respond to sexual advances
3. Clients are blackmailing peers using screen shots from online outreach conversations	A, B, C, D, E	C. Use closed Facebook (or other platform) groups and have a process to verify individuals' identities before they join
		D. Share names/photos of habitual harassers so that they are not engaged in online programming
		E. Have policies that prevent workers from having romantic relationships with clients

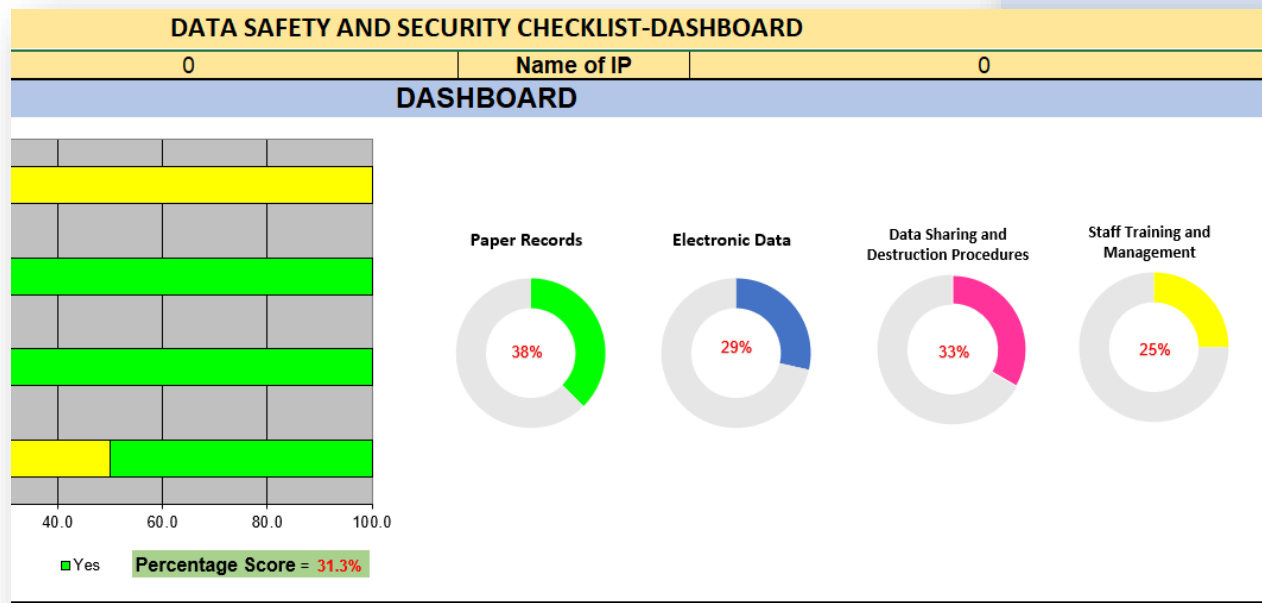


## Additional tools and guidance: Strategic information

EpiC and LINKAGES developed a dashboard for self-assessment and guidance on the security of strategic information

Visit:

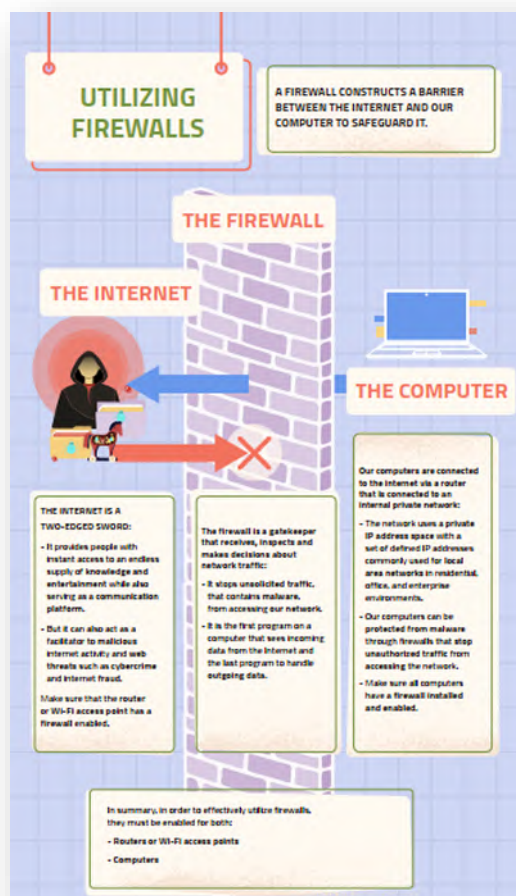
<https://www.fhi360.org/resource/impl-ementer-and-data-security>



# Additional tools and guidance: General online security

- In collaboration with LINKAGES, the Arab Foundation for Freedoms and Equality developed a virtual digital security training that helps both program implementers and beneficiaries use the internet safely.
- The self-paced and live trainings can be found here:

<https://afemena.org/digital-security-sessions/>



# Additional tools and guidance: Secure use of mobile devices and apps

- Supports organizations in the secure use of mobile devices and apps
- Topics:
  - Choosing devices
  - Deploying/managing devices
  - Client privacy and protection
  - Virtual case management
- Website:  
<https://www.fhi360.org/sites/default/files/media/documents/resource-secure-mobile-devices-apps.pdf>

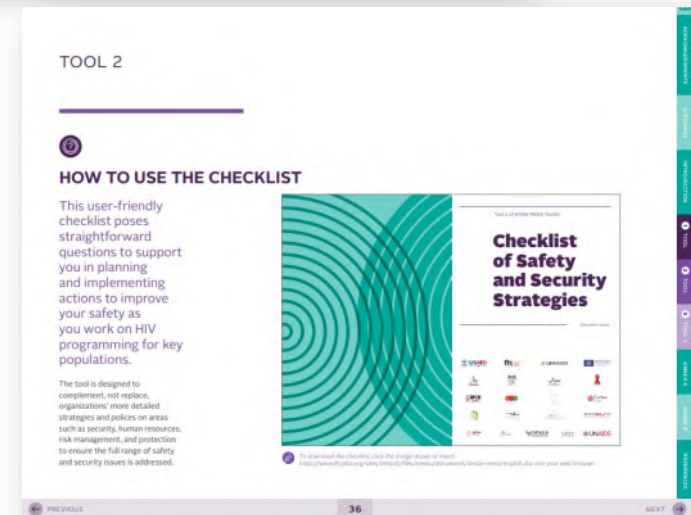
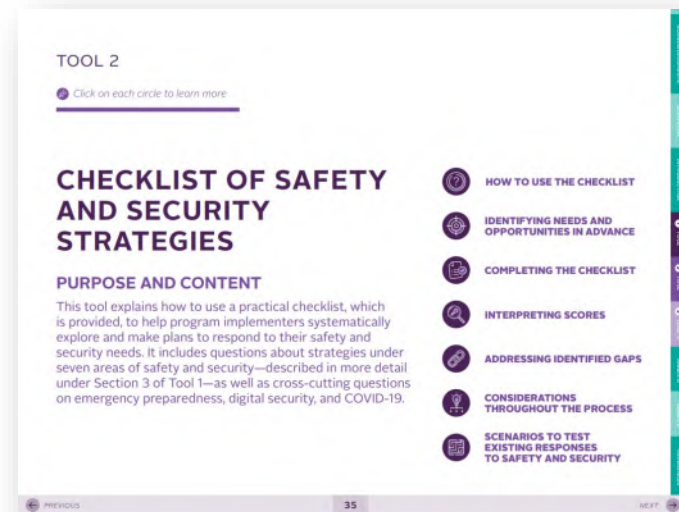




**Review our own  
capacities and plan for  
skill sharing**

# Session Objectives

- Review collective responses to the security assessments (checklists).
- Assign each implementing partner to a skill to be presented in the next session.



The checklist that each partner should fill out is part of the AMAN MENA (Secure in MENA) toolkit. A hyperlink to the checklist can be found at the start of Tool 2 in the toolkit, available in Arabic, English, and French. All three toolkits can be found here:

<https://www.fhi360.org/resource/aman-mena-toolkit>

# Step 1

## Areas of security assessed in the checklist

- A. Cultivating and sensitizing external allies
- B. Influencing public perception of the project or organization
- C. Documenting harms for tracking and advocacy
- D. Protecting offices, drop-in centers, and other physical locations
- E. Keeping workers safe during physical and digital outreach
- F. Developing functional and institutionalized security protocols, including for emergencies
- G. Keeping data and communications safe
- H. Cross-cutting: emergency preparedness, digital safety, COVID-19



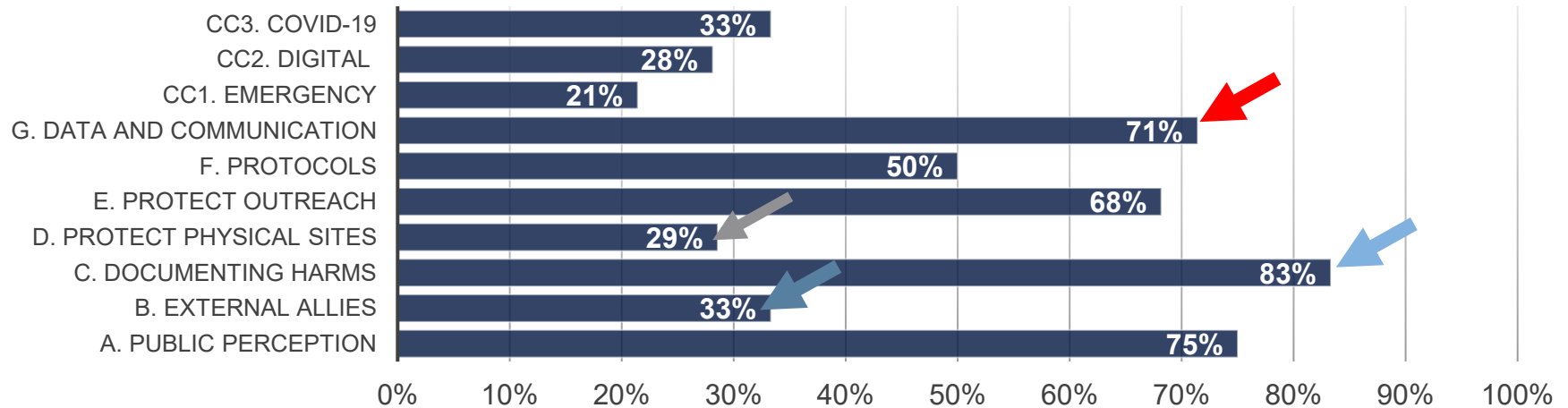
Strategy		Yes	No	Somewhat applicable	Not applicable	Notes and score
<b>C. Documentation of harms for tracking and advocacy</b>						
To be completed by both (1) the organization leading the project and/or the umbrella agency and (2) individual organizations implementing activities (with each organization filling out their own survey)						
23	Does the organization document abuses against its beneficiaries and/or staff?	1				
24	Does the organization keep an anonymized list of security incidents that have affected their operations?		1			
25	Does the organization analyze documented abuses or threats to predict future safety issues or perform advocacy?			1		
26	Does the organization document surges in abuse related to crises such as COVID-19?				1	
	TOTAL	1	1	1	1	
SCORE PART C						50.0%



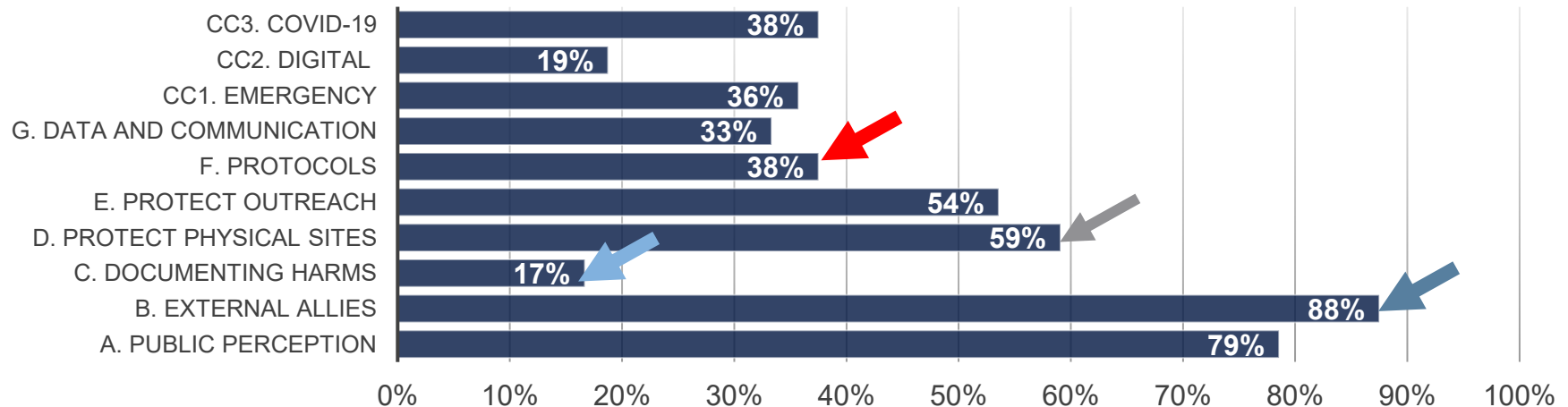


# Activity T (part 1). IP Teaching Assignments

## Scores by Area—Organization 1



## Scores by Area—Organization 2





## Activity T (part 2). IP Teaching Assignments

- Look at the area you will be teaching
- Pick at least one strategy from within this area that you would like to share with others
- Create four slides
  - Title slide: Organization name and topic name
  - How to implement this strategy
  - Any tools to support implementation
  - Results of anecdotal evidence on how this strategy helped
- You will have 10 minutes to present and then 5 minutes for questions
- Presentations will be at X time on Y date



### Assignments:

- ??? = public perception (A)
- ??? = external allies (B)
- ??? = documenting harms (C)
- ??? = protect physical sites (D)
- ??? = protect outreach (E)
- ??? = protocols (F)
- ??? = data and communication (G)
- ??? = emergencies (CC1)
- ??? = digital security (CC2)
- ??? = COVID-19 (CC3)



## Activity T (part 3). Example

- The CSO, “Health for One and All” is assigned to Domain C: Documentation of harms.
- The CSO looks at the strategies under C and chooses at least one to share with the larger team.

Strategy		Yes	No	Somewhat applicable	Not applicable	Notes and score
<b>C. Documentation of harms for tracking and advocacy</b>						
To be completed by both (1) the organization leading the project and/or the umbrella agency and (2) individual organizations implementing activities (with each organization filling out their own survey)						
23	Does the organization document abuses against its beneficiaries and/or staff?	1				
24	Does the organization keep an anonymized list of security incidents that have affected their operations?		1			
25	Does the organization analyze documented abuses or threats to predict future safety issues or perform advocacy?			1		
26	Does the organization document surges in abuse related to crises such as COVID-19?				1	
	TOTAL	1	1	1	1	
SCORE PART C						50.0%



## Day 2 closing



# Session Objective

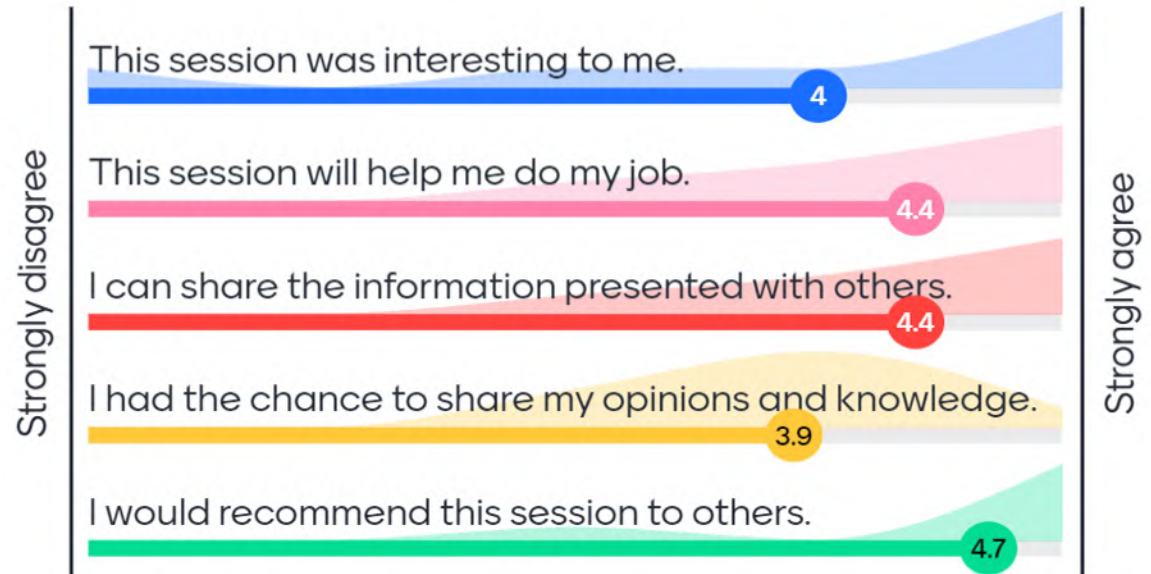
Complete Day 2 evaluation



# Activity U. Day 2 Closing

Go to [www.menti.com](https://www.menti.com) and use the code 88 64 96 0

Please share your opinions about today's session.





---

# Strengthening the Security of HIV Service Implementers Working with Key Populations

A virtual training for  
organizational leadership

---

April 2021

## DAY 3





# Session Objectives

- Share a security strategy assigned to your CSO.
- Ask questions about all presented strategies to gain understanding of implementation, and pros and cons of the strategy.



# Activity V. Implementing partner presentations

- Each should have
  - Title slide: Organization name and topic name
  - How to implement this strategy
  - Any tools to support implementation
  - Results of anecdotal evidence on how this strategy helped





---

# Strengthening the Security of HIV Service Implementers Working with Key Populations

A virtual training for  
organizational leadership

---

April 2021

## DAY 4







## **Day 2 recap and Special Session reflections**



# Session Objectives

- Reflect on strategies presented during the special session.
- Remember the topics covered on Day 2.



## Activity W. Key takeaways

- Thinking of the skills and strategies you learned from your colleagues during the last session, share a few ideas that you plan to use at your organization.



# Activity X. Remembering Day 2

- Menti.com



# Using what you've learned: Security challenge scenarios



# Session Objectives

- Brainstorm what your organization could do if faced with a variety of security challenges.
- Discuss whether the “possible solutions” after each scenario would be appropriate in the local context.



# Eight security incident scenarios

1. Local religious leaders claim that your organization is promoting sin by distributing condoms and lubricants. As a result, there is an increase of physical and verbal abuse against peer educators.
2. A worker reports that he has been harassed by another worker.
3. An outreach worker is arrested while distributing condoms; she is held by police.
4. After an HIV outreach activity at a hot spot, a beneficiary puts photos of the outreach workers and KP members on Facebook and tags them.
5. Your organization's office is raided; police take all the files and computers.
6. A hostile article about your organization is printed in the newspaper. It gives the address of your clinic and includes photographs of two of your clinicians.
7. A beneficiary threatens one of your peer outreach workers with blackmail. The beneficiary says he will tell the outreach worker's parents that the worker is gay.
8. A nurse goes to the home of a man named by an index client. The man responds violently. He attacks the outreach worker (ORW) and gives the ORW several injuries. He also holds the ORW against his will for three hours.



## Activity Y. Using what you've learned

IP name	Case Study
	1
	2
	3
	4

IP name	Case Study
	5
	6
	7
	8

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?

After the group presents their answers, some possible solutions will be shown. The presenting group should respond to the possible solutions, noting whether any possible solutions are inappropriate/irrelevant in their setting or could be good additions to what they already presented.





# Activity Y. Scenario 1

**Local religious leaders claim that your organization is promoting sin by distributing condoms and lubricants. As a result, there is an increase of physical and verbal abuse against peer educators.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?

# Scenario 1 – Possible solutions

- In advance:
  - Work with religious leaders to explain your work. Providing health care to the most vulnerable aligns with the teaching of most major religions. Religious leaders can be powerful advocates for HIV programs.
  - Have a security incident tracking log so that it is clear which areas are seeing increased abuse.
- After the incident:
  - Provide support to impacted peer educators (including mental and physical health care, legal, other psychosocial).
  - Reduce outreach activities in particularly impacted areas, at least temporarily.
  - Report back to the donor with the issue, proposed responses, and any anticipated changes in ability to meet objectives/targets.
  - Ask local health officials to reach out to religious leaders and/or to convene a meeting where it is possible to explain the nature of your work and its alignment with government objectives related to public health.



## The Cairo Declaration of Religious Leaders in the Arab States in Response to the HIV/AIDS Epidemic

We, the Muslim and Christian leaders, working in the field of HIV/AIDS in the Arab world, meeting in Cairo, Egypt from the 28-30 Shawal 1425 H, 11-13 December 2004 AD, in an initiative of the United Nations Development Programme's (UNDP) HIV/AIDS Regional Programme in the Arab States (HARPAS), under the auspices of the General Secretariat of the League of Arab States, and in collaboration with UNAIDS and FHI/Interact, have agreed upon the following:

### First: General Principles

- Due to our realization of the value of every human being, and our awareness of God's glorification of all human beings - notwithstanding their situation, background or medical condition- we, as religious leaders, face the imminent danger of the HIV/AIDS epidemic and have a great responsibility and duty that demands urgent action.
- It is our duty to promote virtue and religious values and enhance people's relationship with their Creator, seeking God through prayers and petitions that He may protect us from this imminent danger and preserve our homeland from it, and that He may grant His grace and favor upon those affected by this disease.
- We encourage them to pray and receive God's help and grace.
- Illness is one of God's tests, anyone may be afflicted by it according to God's sovereign choice. Patients are our brothers and sisters, and we stand by them seeking God's healing for each one of them.

### Second: On Prevention

- The family is the foundation for building and defending society. It is therefore necessary to encourage starting families in accordance with heavenly decrees, and we should remove all obstacles in the way, while emphasizing the prohibition of adultery by all heavenly decrees.
- We emphasize the need to break the silence, doing so from the pulpits of our mosques, churches, educational institutions, and all the venues in which we may be called to speak. We need to address the ways to deal with the HIV/AIDS epidemic, based upon our genuine spiritual principles and our creativity, and armed with scientific knowledge, aiming at the innovation of new approaches to deal with this dangerous challenge.
- We reiterate that abstinence and faithfulness are the two cornerstones of our preventive strategies, but we understand the medical call for the use of different preventive means to reduce the harm to oneself and others.
- We view as impious anything that may cause infection through intention or negligence - as a result of not using all possible preventive means available, in accordance with heavenly laws.
- We emphasize the importance of reaching out to vulnerable groups which are more at risk of being infected by HIV/AIDS and/or spreading it, including commercial sex workers and their clients, injecting drug users, men having sex with men, and those who are involved in harmful practices. We emphasize the importance of diverse approaches and means to reach out to those groups, and although we do not approve of such behaviors, we call on them to repent and ask that treatment and rehabilitation programs be developed. These programs should be based on our culture and spiritual values.
- We call upon the media to abide by ethical codes regarding the material they present.
- We advocate the rights of women to reduce their vulnerability to HIV/AIDS.

### Third: On Treatment and Care

- People living with HIV/AIDS and their families deserve care, support, treatment, and education, whether or not they are responsible for their illness. We call for our religious institutions, in cooperation with other institutions, to provide spiritual, psychological, and economic guidance and support to those in need. We also encourage them not to lose faith in God's mercy, and aspire to a rewarding and productive life, embracing life with courage and faith.
- We reject and emphasize the necessity to abolish all forms of discrimination, isolation, marginalization, and stigmatization of people living with HIV/AIDS. We insist on defending their basic freedoms and human rights.

### Fourth: Addressing other leaders

- As religious leaders we need to reach out to our governments, civil society institutions, NGOs, and the private sector, to seek closer cooperation and greater action in the response to this epidemic.
- We also emphasize the importance of mobilizing other religious leaders' role against the imminent danger of HIV/AIDS in society, particularly in the media and in educational and popular campaigns.
- The need to formulate policies and laws that prevent the further spread of the disease, particularly mandatory marriage check ups before marriage.
- Promote the setting up of guidance and awareness raising centers and facilitate the establishment of charitable organizations to provide care, and support for people living with HIV/AIDS.

<https://www.fhi360.org/resource/cairo-declaration-religious-leaders-arab-states-response-hivaids-epidemic-pdfs-arabic-and>



## Activity Y. Scenario 2

**A worker reports that he or she has been harassed by another worker.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



## Scenario 2 – Possible solutions

- In advance:
  - Create codes of conduct for staff; develop policies to address grievances that ensure multiple levels of accountability, such as complaints directly to the board, and socialize all workers on the policies as part of on-boarding
- After the incident:
  - Follow existing policies to address the harassment without putting the victim at risk of retaliation OR develop new policies if no relevant policies exist
  - Retrain workers on the code of conduct (or provide an initial training)
  - Offer mental health support to the person who was harassed



## Activity Y. Scenario 3

**An outreach worker is arrested while distributing condoms and is being held by police.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



# Scenario 3 – Possible solutions

- In advance:
  - Work with local authorities to receive permission for all outreach activities, and train senior and front-line law enforcement officers on their role in the HIV response, including creating an enabling environment for outreach activities.
  - Train outreach staff to explain the nature of their activities to law enforcement and provide them with official documentation (such as ID cards or letters from local authorities or the Ministry of Health) describing their purpose.
  - Identify lawyers who can support the organization as needed if issues arise.
- After the incident:
  - Call allied lawyers or an in-house attorney to follow up immediately (if there is no funding for a lawyer and no opportunity to engage a lawyer pro bono, reach out to Dignity for All [focused on LGBT communities], Frontline Defenders, The Lifeline Embattled CSO Assistance Fund, or other funds for support).
  - If contacts with the police exist, call these individuals to discuss next steps.
  - If there is a desire to make the issue more publicly visible (for example, by activating allies), ensure that this case is thoroughly investigated before taking this step.



## Activity Y. Scenario 4

**After an HIV outreach activity with KP members, a beneficiary posts photos of the outreach workers and community members on Facebook and tags them.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



# Scenario 4 – Possible solutions

- In advance:
  - Inform people who come to any events whether the space is photo-friendly (this can also help beneficiaries who see others taking photos to remind them of policies or report them as needed).
- After the incident:
  - If the photos are posted without negative intent, reach out to the person to take them down and explain the importance of not posting such photos in the future.
  - If an individual knowingly violated clear policies or will not take down photos, do not allow them to participate in future events.
  - Report the individual to Facebook administrators who can suspend their profile.
  - Notify those who were identified and explain the steps being taken to address the issue. Provide them with support as needed if the posting causes emotional or physical abuse.





## Activity Y. Scenario 5

**The organization's office is raided by the police, and police take all the files and computers.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



# Scenario 5 – Possible solutions

- In advance:
  - Protect all technology that includes stored information with passwords and encryption.
- After the incident:
  - Create a plan that describes what will happen to support those named if data are leaked.
  - Reach out to senior allies within the police force to give you advice on how to proceed. For example, clarify what will be done with these materials and encourage them not to misuse or share medical files and other personal information.
  - If the seizure was not legal, consider contacting a lawyer to challenge materials taken without a warrant.
  - Report back to the donor with the issue, proposed responses, and any anticipated changes in ability to meet objectives/targets.



## Activity Y. Scenario 6

**A hostile article about your organization is printed in the newspaper; it gives the address of your clinic and includes photographs of two of your clinicians.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



# Scenario 6 – Possible solutions

- In advance:
  - Connect with local authorities and law enforcement to explain, in conjunction with a Ministry of Health (MOH) official, the nature of your organization's activities.
  - Register your organization.
  - Work to build relationships with powerholders, such as religious leaders or local authorities, who can defend your organization.
  - Have a clear policy that describes how your organization interacts with journalists and use press statements instead of interviews. In an interview, comments made by your organization's staff or members may be distorted or taken out of context.
- After the incident:
  - Increase security at the clinic.
  - Inform allied local authorities of the issue and ask for their support in case violence against the organization or individual providers occurs.
  - Support the clinicians to relocate briefly or change their responsibilities (such as only having them work during day shifts or stop doing community-based activities) if they believe they will be in danger.
  - Have the MOH write an article clarifying the role of the organization and its importance to the health of the community.



## Activity Y. Scenario 7

**A peer outreach worker at your organization is blackmailed by a beneficiary who threatens to tell the worker's parents that the worker is gay.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



# Scenario 7 – Possible solutions

- In advance:
  - Have a clear code of conduct for program participants that includes expectations of confidentiality and describes consequences of a failure to meet these expectations.
  - Talk to peers and other staff about the risks they may face, including in their personal lives, because of their work and help them decide whether they wish to take on a role that may increase the chances their families or friends will discover their KP-status if it is not already known.
- After the incident:
  - Support the mental health of the worker by providing active listening and linking them to a counselor, if desired.
  - Offer to help facilitate a conversation with the worker and their parents, if desired.
  - Explain the local legal context (for example, is the beneficiary's action illegal) and options to the worker; these include no action (blackmail is often not carried out) and blocking the beneficiary on social media and phone. Once the worker decides on an option, provide support as relevant as they carry out their choice.
  - Prevent the beneficiary from returning to any future program events.



## Activity Y. Scenario 8

**An outreach worker (ORW) goes to the home of a man named by an index client. The man responds violently. He attacks the ORW and gives the ORW several injuries. He also holds the ORW against his will for three hours.**

- What can you do now?
- What could you have done, before this issue occurred, to mitigate or prevent the harms caused?



# Scenario 8 – Possible solutions

- In advance:
  - Offer several index testing modalities (with IPV screening to inform selection).
  - Have clear guidance on when home visits should occur (e.g., person visited must give consent in advance), and how these visits should be carried out (e.g., always in pairs).
  - Have a system in place to track workers conducting outreach (e.g., know where they are going, expected arrival and return; consider tracking using GPS).
  - Offer medical insurance to workers and/or develop a system for them to receive free medical care if injured on the job.
- After the incident:
  - Have the supervisor alert leadership of the ORW's late return.
  - Connect the ORW to free treatment of injuries.
  - Provide the ORW with psychological resources.
  - Contact police to file a report against the perpetrator (if in line with ORW's wishes).
  - Place potential client on a “no contact” list for future reference.





## Activity Z. Reflections on the Scenarios

**Q:** Thinking about the eight scenarios we have just discussed, why are actions taken before the security challenge so important?

**A:** There are three major reasons:

1. When you have a security plan in place before a security challenge occurs, you can respond more quickly and in a more organized/efficient way than if you try to develop a plan while in the middle of a crisis.
2. Security planning puts structures and relationships in place that prevent security challenges from happening or makes them less harmful if they do occur.
3. It is much less costly (time and money) to prevent a security incident than to respond to one.



## Final reflection on security scenarios

If your organization has specific concerns that were not covered here, write each one down. Then, do this exercise using those concerns.

Plan now to avoid negative consequences later!

**~~UN~~PREPARED**



# Risk assessment formula



# Session Objective

Become familiar with the formula for determining the likelihood that a given harm will occur.

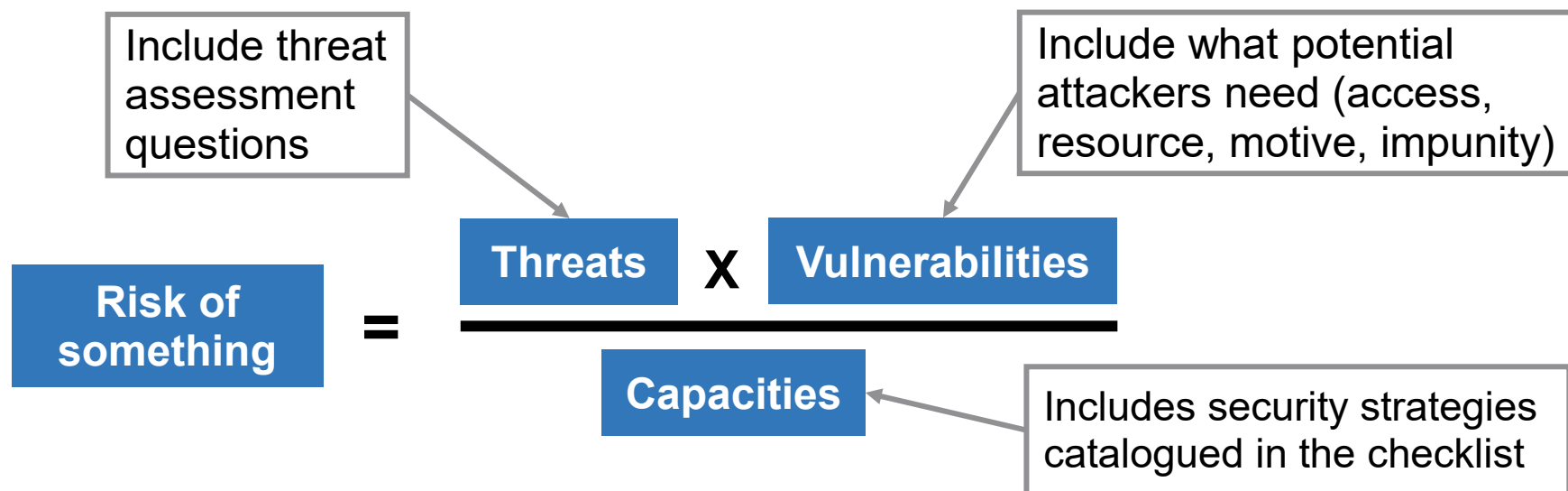


# Trade-offs

- Limiting an attacker's access, resources, and motivations can have trade-offs for you as an individual and as an organization.
- How do you decide what vulnerabilities to accept?

# Take action to make the risk low

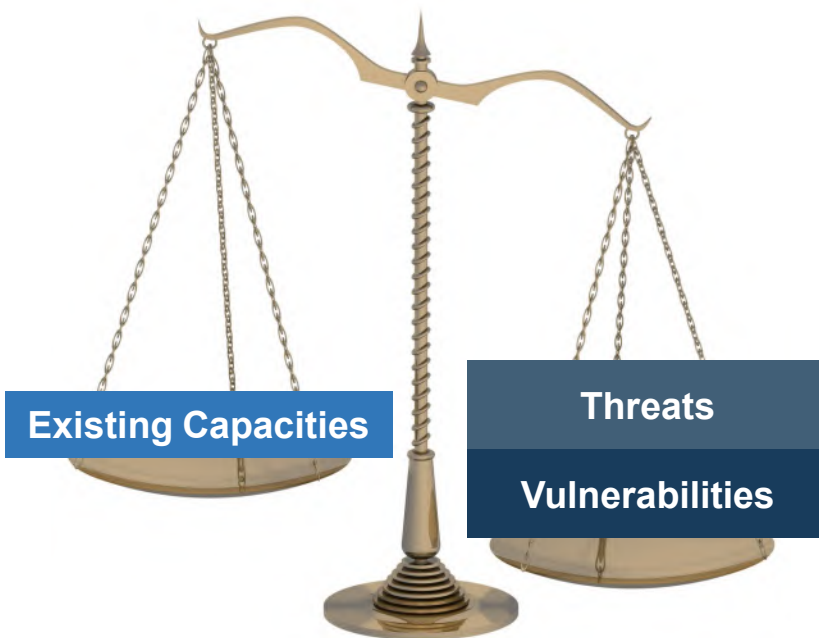
- **Threats** – you can assess these indications and can perhaps change them over time, but you have limited control over them (external)
- **Vulnerabilities** – inherent to you/your community; some you can control, others you cannot (internal)
- **Capacity** – what you constantly want to work to increase (internal)



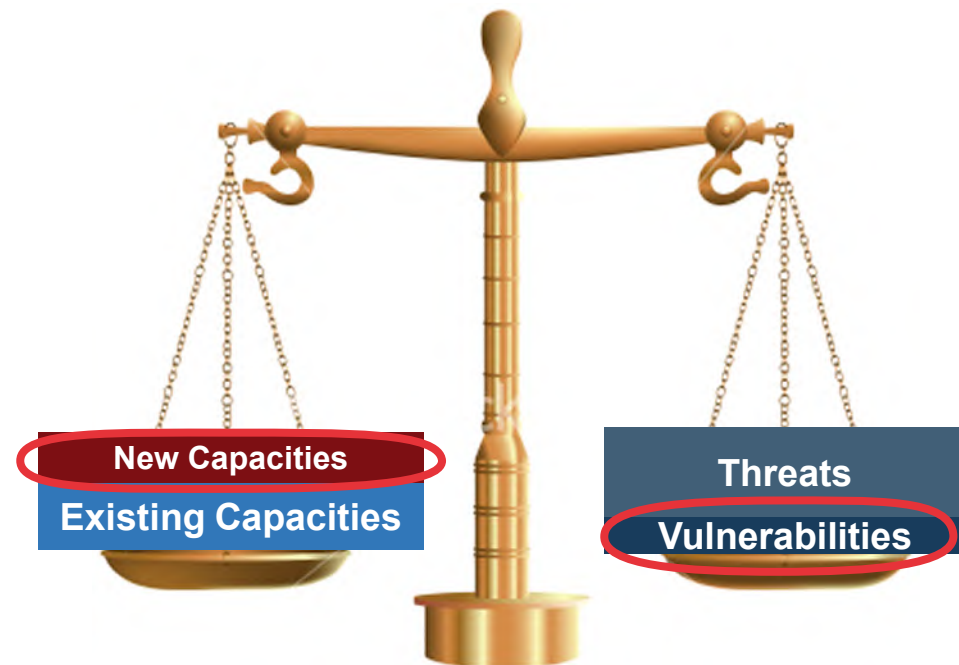


# We want to go from this...

To closer to this



Threats and vulnerabilities far outweigh capacities



Capacities are equal to or greater than threats and vulnerabilities



# Formula for calculating risk

$$\text{Risk of something} = \frac{\text{Threats} \times \text{Vulnerabilities}}{\text{Capacities}}$$

$$\text{Risk of something} = 25 = \frac{\text{Threats} = 5 \times \text{Vulnerabilities} = 10}{\text{Capacities} = 2}$$

$$\text{Risk of something} = 20 = \frac{\text{Threats} = 5 \times \text{Vulnerabilities} = 8}{\text{Capacities} = 2}$$

$$\text{Risk of something} = 8 = \frac{\text{Threats} = 5 \times \text{Vulnerabilities} = 8}{\text{Capacities} = 5}$$

Realistically, risk never goes to zero and situations change quickly. This tool gives you a **relative sense** of how likely different harms are so you can compare one risk to another and compare your own level of risk over time.





# Risk Assessment Example

$$\text{Risk of something} = \frac{\text{Threats} \times \text{Vulnerability}}{\text{Capacity}}$$

- Pick a **specific risk** (location, activity, person)
  - Our CSO is worried that our peer ORWs will be physically assaulted during outreach
- Consider **threats** that make the risk likely
  - Verbal abuse, including threats of physical violence, occurred in the past; the perpetrators are often the bar owners. Verbal threats are increasing.
- Name your **vulnerabilities**
  - Outreach is done by sex workers; it occurs at night; transport is on foot
- Name your **capacities**
  - Peer outreach workers wear ID cards that show they are connected to the Ministry of Health and include a phone number to reach a locally trained police officer; peers go out in pairs; peers have phones with pre-paid airtime in case they encounter issues



# Activity AA. Risk Assessment Example

$$\text{Risk of something} = \frac{\text{Threats} \times \text{Vulnerability}}{\text{Capacity}}$$

- Pick a **specific risk** (location, activity, person)
  - Our CSO is worried that the ORWs will be physically assaulted during outreach
- Consider **threats** that make the risk more or less likely
  - Verbal abuse, including threats of physical violence, occurred in the past; the perpetrators are often the bar owners.
- Name your **vulnerabilities**
  - Outreach is done by sex workers; it must occur at night; transport is on foot
- Name your **capacities**
  - Peer outreach workers wear ID cards that show they are connected to the Ministry of Health and include a phone number to reach a locally trained police officer; peers go out in pairs; peers have phones with pre-paid airtime in case they encounter issues

**Discussion: What could you do to reduce vulnerabilities and increase capacities?**



# Activity AA. Risk Assessment Example

$$\text{Risk of something} = \frac{\text{Threats} \times \text{Vulnerability} - 1}{\text{Capacity} + 4}$$

- Pick a **specific risk** (location, activity, person)
  - Our CSO is worried that the ORWs will be physically assaulted during outreach
- Consider **threats** that make the risk more or less likely
  - Verbal abuse, including threats of physical violence, occurred in the past; the perpetrators are often the bar owners.
- Name your **vulnerabilities**
  - Outreach is done by sex workers; it must occur at night; transport is ~~on-foot~~ **by taxi**
- Name your **capacities**
  - Peer outreach workers wear ID cards that show they are connected to the Ministry of Health and include a phone number to reach a locally trained police officer; peers go out in pairs; peers have phones with pre-paid airtime in case they encounter issues; **peers have a noncontroversial message to describe their work; peers' whereabouts are tracked via logbook and GPS; peers have pre-identified safe havens in each neighborhood they work in; sex workers are accompanied by a known and respected escort from the area**



# Security planning



# Session Objectives

- Recognize the elements of a security plan and practice using the template to develop your own.
- Identify your top three risks and create a security plan for each by considering vulnerabilities, existing capacities, and needed capacities.



# Security planning

Risk (of something): **A break-in at the clinic with client records stolen**

Threats	Vulnerabilities	Existing capacity	Required capacity
<b>High</b> <ul style="list-style-type: none"><li>• Outreach workers have been followed back to clinic by yelling groups who say we promote homosexuality</li><li>• Threatening messages graffitied onto clinic</li></ul>	<ul style="list-style-type: none"><li>• We are in a neighborhood with little street traffic in the evenings</li><li>• We do not have any security guards at the clinic after 5 pm</li><li>• We don't have a way to monitor visitors during the day</li><li>• Staff do not always lock up patient charts</li><li>• Windows and doors do not have bars; can be broken with rocks</li></ul>	<ul style="list-style-type: none"><li>• We have a security guard while the clinic is in operation (9 am–5 pm)</li><li>• We have the USAID and MOH logo on our sign</li><li>• We have introduced ourselves and explained our work to senior law enforcement officers working in the district</li><li>• We have locked cabinets to store all paper client records</li><li>• We use UICs and keep mostly encrypted electronic information</li></ul>	<ul style="list-style-type: none"><li>• Visitor monitoring logs</li><li>• Retraining for all staff on safe document storage (clean desk policy)</li><li>• Talk to landlord about the nature of our work</li><li>• Install physical security measures for windows and doors</li><li>• Create log for security challenges to track trends; consider using it to advocate with donor for funds for increased security presence</li></ul>



# Security planning with low cost/no cost options ←

Risk (of something): A break-in at the clinic with client records stolen			
Threats	Vulnerabilities	Existing capacity	Required capacity
<b>High</b> <ul style="list-style-type: none"><li>• Outreach workers have been followed back to clinic by yelling groups who say we promote homosexuality</li><li>• Threatening messages graffitied onto clinic</li></ul>	<ul style="list-style-type: none"><li>• We are in a neighborhood with little street traffic in the evenings</li><li>• We do not have any security guards at the clinic after 5 pm</li><li>• We don't have a way to monitor visitors during the day</li><li>• Staff do not always lock up patient charts</li><li>• Windows and doors do not have bars; can be broken with rocks</li></ul>	<ul style="list-style-type: none"><li>• We have a security guard while the clinic is in operation (9 am–5 pm)</li><li>• We have the USAID and MOH logo on our sign</li><li>• We have introduced ourselves and explained our work to senior law enforcement officers working in the district</li><li>• We have locked cabinets to store all paper client records</li><li>• We use UICs and keep mostly encrypted electronic information</li></ul>	<ul style="list-style-type: none"><li>• Visitor monitoring logs</li><li>• Retraining for all staff on safe document storage (clean desk policy)</li><li>• Talk to landlord about the nature of our work</li><li>• Install physical security measures for windows and doors</li><li>• Create log for security challenges to track trends; consider using it to advocate with donor for funds for increased security presence</li></ul>





# Activity BB. Local Example

Risk (of something): XXXX			
Threats	Vulnerabilities	Existing capacity	Required capacity
<ul style="list-style-type: none"><li>• XXXX</li><li>• XXXX</li></ul>	<ul style="list-style-type: none"><li>• XXXX</li><li>• XXXX</li></ul>	<ul style="list-style-type: none"><li>• XXXX</li><li>• XXXX</li></ul>	<ul style="list-style-type: none"><li>• XXXX</li><li>• XXXX</li></ul>





# Activity CC. Your Priority Risks

1. Brainstorm your organization's biggest security risks
2. Select your top three risks
3. Develop a security plan for each of your three biggest risks
  - Consult the checklist you completed to understand your current capacities and to get ideas for what more can be done
4. Complete the security plans and send them to **XXXXX** by **XXXXX** for feedback



# Next steps



# Session Objectives

- Discuss opportunities for immediate no and low-cost action, continued cross-CSO learning, linking security activities into ongoing violence prevention and response, and seeking international support.
- Identify action steps to finalize and build buy-in for security plans at each CSO.



# Finalizing and funding plans

- Finalizing security plans can include
  - Getting buy-in from others at your organization
  - Asking other stakeholders what specific commitments they will make (landlords, LINKAGES/EpiC, Ministry of Health, etc.)
- Many actions will be no cost or very low cost
  - Those that require funding should be documented to help inform future COP planning and opportunities from other funders



# Activity DD. Action Planning

- After completing your security plans, select from the capacities that you need to build.
- Pick 10.
- Fill out the action plan and return it to XXXXX.
- If one of your plans is to roll this training out to a wider group at your organization, develop your own policies and standard operating procedures on security **before** that training.

	Top 10 Required Capacities to be Pursued	Requires additional monetary resources? (Y/N)	Time capacity will be fully implemented	Main person(s) responsible
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

# Opportunities for Support (funding)



DIGNITY  
FOR ALL



**f** FRONT LINE  
DEFENDERS

**URGENT ACTION FUND**  
FOR WOMEN'S HUMAN RIGHTS

# New opportunities during COVID-19

<https://outrightinternational.org/outright-covid-19-global-lgbtq-emergency-fund>

## Funding can cover:

- Food scarcity, medium- and long-term livelihood generation
- Movement resilience
- Combating violence: (GBV, domestic violence, and family violence), can include mental health support
- Human rights violations documentation

A NEW CALL  
FOR PROPOSALS  
TO THE  
**COVID-19  
GLOBAL LGBTQ  
EMERGENCY  
FUND**  
IS NOW OPEN





# Reflections and closing





# Session Objective

Share thoughts on and evaluate the workshop;  
provide closing reflections.



## Activity EE. Evaluation and Post-Test

- An evaluation of our training can be found here: [XXXXXXX](#)
- The post-test can be found here: [XXXXXXX](#)



# Activity FF. In Your Own Words

Go to [www.menti.com](https://www.menti.com) and use the code 89 82 66 6

Share a word or short phrase that describes how you are feeling at the end of this TOT.

 Mentimeter



A word cloud of responses from participants, with words of varying sizes and colors (blue, green, yellow, red, purple) arranged in a circular pattern. The words include:

- excited
- informed
- useful
- enlightened
- capacitated
- and cautious
- learned a lot
- can help cso staffs
- help peers and providers
- enlightened with to do's
- the was good and relevant
- confident about the topic
- will reduce vulnerability
- curious to learn more
- informative
- educative
- happy to roll it out
- very knowledgeable
- and risk free
- training is relevant
- satisfied
- an eye opener
- will increase our capacit

9



# Acknowledgments

