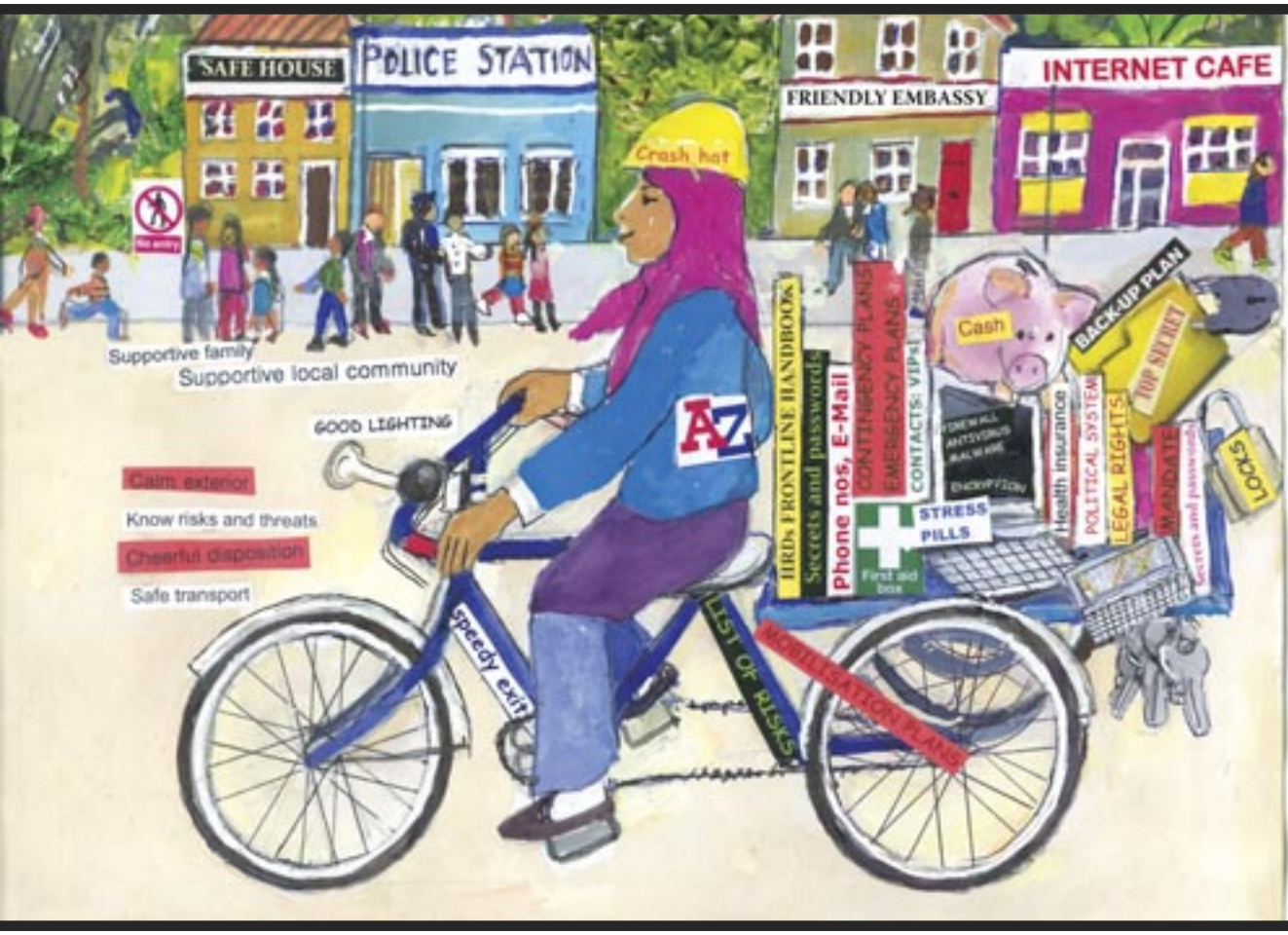
WORKBOOK ON SECURITY:

PRACTICAL STEPS FOR HUMAN RIGHTS DEFENDERS AT RISK



FRONT LINE DEFENDERS

CHAPTER 5: CREATING SECURITY PLANS

> ***" I thought that making a security plan would be a big undertaking. Yes, it can be big, but some of it you can develop as you learn. It need not be complicated."*** **HRD, Middle East**
>
> ***"I travelled from South Africa to run a workshop for Human Rights Defenders in Liberia when we thought the war was over. One night we heard machine gun fire and mortars in the nearest village. I had no plan for what to do. Now I know better..."*** **HRD, Africa**
>
> ***"Putting together and implementing a security plan saved my life."*** **HRD, Americas**

In this Chapter we will look at three different strategies for considering security: the acceptance strategy, the protection strategy and the deterrence strategy. We will then look at how to create security plans - for yourself and for your organisation.

Introduction:

This is the final phase of this Workbook. Now you can bring together the learning from the previous tools you have used – Context Analysis, the Risk Formula, the Risk Matrix, questions for threat analysis, and your plans for dealing with stress.

Three security strategies

First, we will look at **three types of approaches to security**. You and / or your organisation may naturally or deliberately have a policy or preference for one type of strategy, but it is useful to look at all three and consider their attributes.

Acceptance strategy: an approach which involves negotiating with all actors – the local community, the authorities etc, to gain acceptance and ultimately support for the organisation's presence and work. Although this requires careful planning and can be labour-intensive, it may be the most effective strategy in the longer term to reduce threats. This approach usually entails high visibility, so in times of great threat it is sometimes more difficult to adapt to being more low profile.

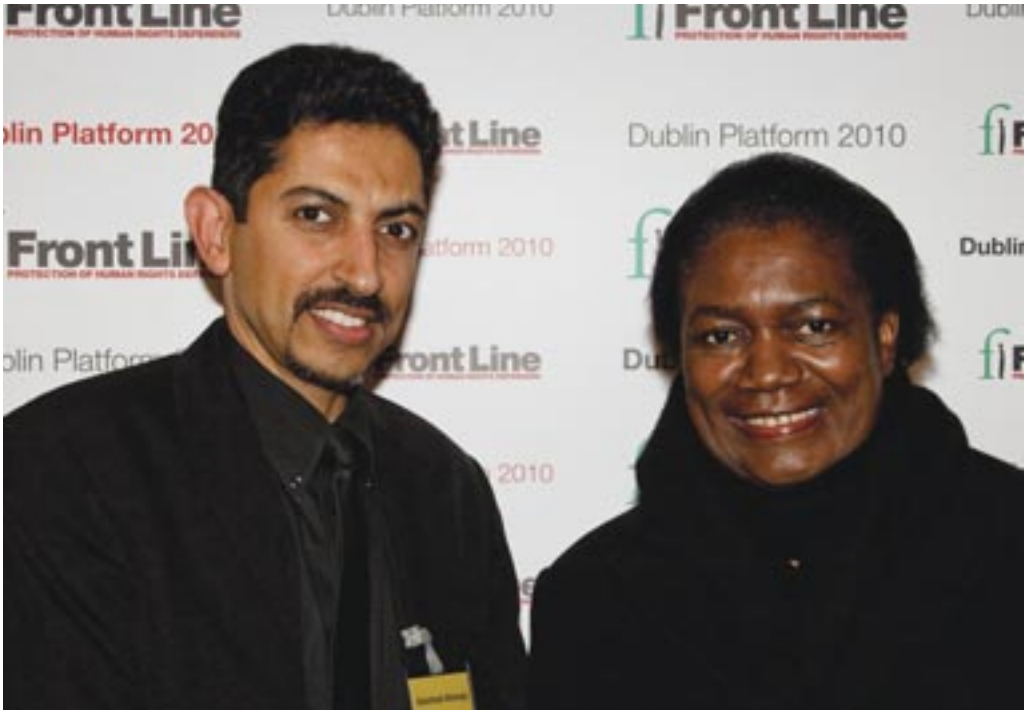
"Making ourselves more visible can be one of the best protection activities. When we meet leaders of regional or international organisations, we insist on having our photo taken with them. We display these photos at our office for everyone to see."
HRD, Asia

"I go fishing with an old school friend, who now works in a government ministry. He tells me a lot of useful information in this relaxing environment."
HRD, Eastern Europe

Protection strategy: an approach which emphasises security procedures and protective elements. Impact is mainly on reducing vulnerabilities. Can of course be used in conjunction with the other two strategies to strengthen protection.

Deterrence strategy: an approach which relies on counter-threats for protection. For example, if threatened, an organisation might react by taking a legal case out against the person issuing the threat, or by publicising the threat, or responding to the perpetrator by explaining the consequences of carrying out the threat – such as international condemnation. This approach should only be used if you have accurate information and powerful allies.

When you are developing your security plans, consider how elements of acceptance, protection and deterrence can expand the menu of options you have at your disposal.



UN Special Rapporteur on HRDs Margaret Sekaggya with Abdulhadi Al Khawaja – currently in prison in Bahrain

Production of Security Plans

We are now going to consider how to produce Security Plans. In human rights organisations where the HRDs are at risk, an organisational security plan will help to protect the workers and allow them to do their work more effectively. If your organisation acknowledges and plans for dealing with the risks, the staff and/or members will feel more supported and have increased allegiance to the organisation and its important work.

We will start however, by considering a Security Plan for an individual. This is for a HRD working on their own. A HRD working in a human rights organisation might also find it useful to have their own individual security plan but generally it will be more effective, for the individual and the organisation, to have an organisational security plan discussed and agreed collectively. Although each individual has unique attributes (such as gender, sexual orientation, age, experience, position in organisation, location of home etc) which make them more or less at risk, individuals will generally make better security plans when drawing on the different experience and perspectives of different members of the group.

Also, where there is an organisational commitment and culture of security the individual is more likely to adhere to agreed security measures. The risk of individual security plans is that they become personal good intentions that get thrown out when things are hectic.

There is also a risk in many organisations that the more high profile and experienced HRDs take all the responsibility for security planning and management in a way which does not build the capacity of other members of the group and can leave the organisation paralysed if the experienced leader is removed. However, an Organisational Security Plan may not cover at all, or may not cover fully, reducing risks in your personal life so it can be helpful to develop a Personal Security Plan as well. And developing a Personal Security Plan can also be good preparation for a discussion on an Organisational Security Plan.

A WHRD, for example, whose husband feels threatened by her high profile and is becoming violent towards her, will have to consider in her Personal Security Plan how to deal with the increasing threat from within the home.

Then we will look at the process for producing an Organisational Security Plan and its contents.

If your organisation does not have an effective Security Plan, you can use this Workbook to assist your organisation to develop one. If your organisation is resistant to creating an Organisational Security Plan or it has a plan but it is not effective, see Appendix 15, *Overcoming Resistance to Security Planning*.

1. Producing a Personal Security Plan

Reminder: Did you identify factors, as suggested in Chapter 1 of what makes you feel secure and what makes you feel insecure? If yes, review this now. Some of the items you identified may become part of your plan. You should by now have more items to add to increase your feeling of security.

Your Personal Security Plan can comprise security policies and procedures and contingency plans You can begin your Personal Security Plan by focusing on two or three risks you face (which you wrote down on Fig 3.1 and perhaps also Fig 3.2). Perhaps you face more than three risks, in which case you can return to include the others later, but focusing on two or three to begin with makes the process easier to manage. Most HRDs choose to focus on two or three risks which are medium to very high impact, and medium to very high probability (see Chapter 2).

If you have not already done so, plot each of the risks on the Risk Matrix (Fig 3.5) by assessing how likely they are to happen (their probability) and what impact they will have on you if they do in fact occur. To do this you will use your experience and knowledge of the political situation. It is a subjective assessment.

HRDs at the Dublin Platform networking with Navi Pillay, UN High Commissioner for Human Rights

For the risks you have identified as moderate to very likely probability, you can draw up an Action Plan. This aim of this is to reduce the likelihood of the situation occurring.

Opposite is a very simple example - it is not meant to be a blueprint for your situation. You can look at more examples of points to consider including in the Appendices. However, you are the person best placed to know what will be most effective, given your unique situation of capacities and vulnerabilities.

My Personal Security Plan

ACTIVITY

Risks:

Risk 1 . . . . . .

Probability . . . . . Impact . . . . . .

Threat assessment: . . . . . .

Vulnerabilities: . . . . . .

Capacities: . . . . . .

Action Plan:

1. . . . . .

2. . . . . .

3. . . . . .

4. . . . . .

5. . . . . .

Risk 2 . . . . . .

Probability . . . . . Impact . . . . . .

Threat assessment: . . . . . .

Vulnerabilities: . . . . . .

Capacities: . . . . . .

Action Plan:

1. . . . . .

2. . . . . .

3. . . . . .

4. . . . . .

5. . . . . .

ACTIVITY CONTINUED:

My Personal Security Plan

Risks:

Risk 3 . . . . . .

Probability . . . . . Impact . . . . . .

Threat assessment: . . . . . .

Vulnerabilities: . . . . . .

Capacities: . . . . . .

Action Plan:

1. . . . . .

2. . . . . .

3. . . . . .

4. . . . . .

5. . . . . .

Example only:

Personal Security Plan

Risk = Arrest in the context of police search of home and confiscation of papers / phone/ laptop
Probability of this happening: medium to high – other HRDs have been targeted in this way recently.
Impact if it happens: medium to high for myself, my family and my organisation
Threat assessment: Police usually raid homes in the early hours of the morning
Vulnerabilities:
- There is no due legal process - there will not be a search warrant or right to have a lawyer present
- We deal with sensitive information in my organisation
- My young children live at home

Capacities:
- Ability to plan (thinking through how you can best respond in advance reduces the losses you could incur)

Action:
1. Discuss the risk with my spouse and tell him who to call if the police arrive. (possibly getting colleagues / friends to witness the search if their presence will not put them at risk of arrest too) and who to call afterwards (eg human rights organisations)
2. Arrange for the children to sleep at their Aunt's at times of heightened risk
3. Investigate possibility of CCTV in home to record event
4. Be aware of my rights in detention so I can request them authoritatively (even though they probably won't be granted)
5. Have a lawyer briefed in case I am allowed access to a lawyer
6. Do not store sensitive work information at home
7. Delete sensitive information from computer and phone
8. Ensure all my personal affairs (taxes etc) are in order so that they cannot become a pretext for a political prosecution)

Next, for any risks you face which have high to very high impact on you, you can draw up an Action Plan and a Contingency Plan. See overleaf for a short example based on the experience of HRDs who have been faced with kidnap by tribal groups.

"The security forces came to arrest me at our office. They wanted to do it quietly. I quickly sent a text message to a whole group of people with a pre-arranged code about an urgent meeting. When 50 people arrived, the security forces left."
HRD, Asia

Personal Security Plan

Risk = Kidnap
Probability of this happening: moderately likely - HRDs who travel in rural areas are sometimes kidnapped by tribal groups. I frequently travel in rural areas for my work.
Impact if it happens: Medium to Very High - some victims of kidnaps have been well-treated; others have been assaulted, raped and killed.
Threat assessment: Perpetrators are from different tribal groups, depending on the area, and are heavily armed
Vulnerabilities:
- I need to travel to areas where kidnaps occur and I could be easily identified as non-local

Capacities:
- Our organisation has funds for security
- Ability to plan for this (thinking through how you can best respond in advance reduces the likelihood)

Action Plan:
1. Consider whether it is safer to travel in a more high profile way – eg publicly, maybe with a high profile person, perhaps in a secure convoy, OR
2. Travel in a low profile way, perhaps on public transport, wearing clothes worn by local people in the area
3. If possible travel with a colleague / companion who will act as some protection, for example because s/he is known in the area / speaks the local language etc
4. Do not travel without having a trusted local contact at my destination
5. Leave schedule of travel plans with designated colleague, and check in with her/him twice a day to confirm all is OK
6. Prepare list of contact details of village elders who have worked with our organisation and could negotiate with the kidnappers – take it with me and also leave a copy with the organisation
7. When travelling, do not follow specific routines
8. In villages, only go where trusted local contact recommends
9. Be aware of what is going on around me at all times (situation awareness) and take action immediately if something does not appear normal.

Contingency Plan:
If I am kidnapped:
1. Stay calm and quiet – especially in the initial process of being kidnapped when the kidnappers will be most nervous and prone to violence
2. Do not try to escape – unless the kidnappers clearly intend the worst
3. Ask to send a message immediately to my organisation
4. Try to gain the kidnappers' respect and build rapport with them
5. Obey orders without appearing servile, but also ask for improved treatment
6. Take care of health: eat and exercise
7. Keep busy by memorising details, descriptions of perpetrators, possible locations, number of days as they pass, etc.
8. Know my organisation has a plan for negotiating for my release and they will do everything in their power to achieve that.

"I was kidnapped by agents of the military. I realised the location I was in because of the address of the shop on the take-away food wrapper. I was blindfolded and questioned. When I was finally released I was later able to identify one of the perpetrators by linking the smell of his aftershave with his voice. Although this information was not enough to charge the perpetrator, consciously collecting this information at the time gave me a sense of control."
HRD, Asia

Note that Appendix 9 also contains a check list on detention / abduction, with some more suggestions.

Security plans are key building blocks for your security situation. But they may not cover every eventuality. Create a habit of considering "what would I do now if (a certain event happens)?" which develops your capacity to react to both the anticipated, but also the unexpected.

Security plans and procedures are valuable tools, but they also have to be balanced by situational awareness, common sense and good judgement.

2. Producing an Organisational Security Plan

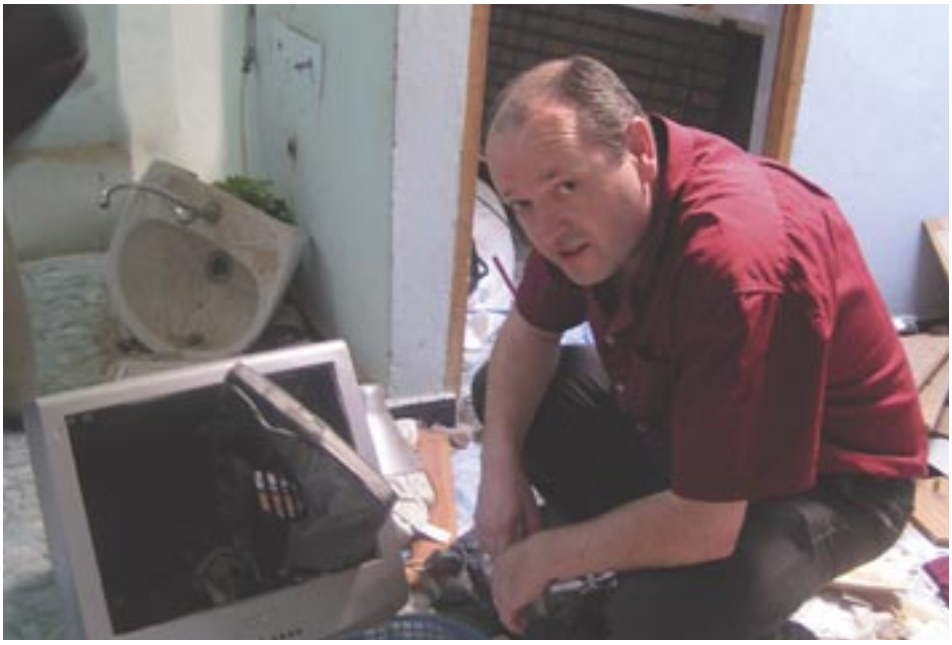
First we will look at the process we recommend for producing the Organisational Security Plan, then at the contents.

The legal responsibility for staff may differ from state to state. Be aware what the legal position is in your country and include Board members in your discussions as appropriate.

2.1 Process of producing an Organisational Security Plan

We recommend you allow a day for the initial discussion. For equipment, you will need a flip chart and paper.

2.1.1 Bring together all your trusted colleagues to **discuss and list the risks you face** as an organisation and as people working within the organisation. Including as many staff as possible in this discussion will begin to build security awareness and commitment to adhere to security measures. Support staff such as the receptionist and driver may not be the most at risk, but they may be the first to spot security incidents. Encourage everyone to contribute and consider each contribution seriously.

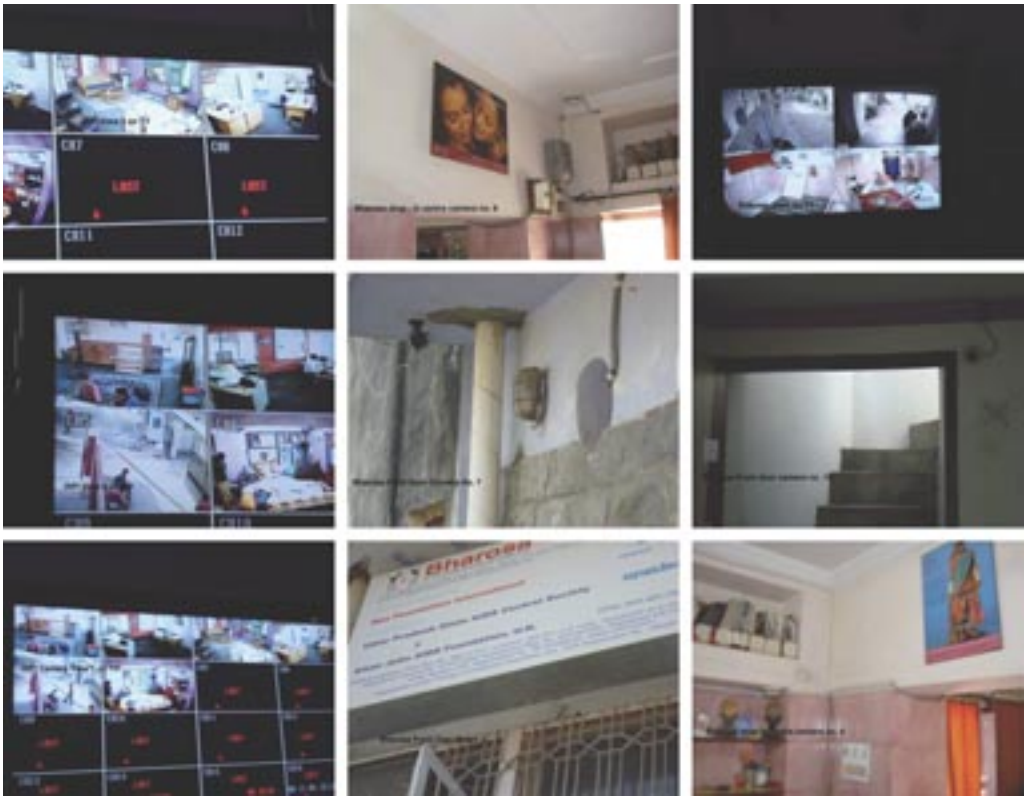


Aftermath of police raid, Western Sahara

Include also in your discussions the way in which you work with groups and individuals - survivors of violence, witnesses etc – and the risks they may face because of contact with you. (You may decide to have a meeting later with representatives of these groups and individuals to check with them the viability of your security plans as they relate to them.)

2.1.2 Prioritise the risks using the Risk Matrix. For each risk, try to find agreement on how probable the risk is and what its likely impact will be – for the people concerned and for the organisation. Log these on a copy of the Risk Matrix. Most organisations would choose to focus on those risks which are medium to high impact, and medium to high probability. In your discussions participants may also identify easy, low cost options for dealing with lower risks. These suggestions should be accepted and implemented if possible but do not lose sight of the most important risks.

2.1.3 Group the risks. So, for example, if your office is vulnerable to burglary and physical attack of the premises, create a category of 'risks to office security' (but write an explanatory sentence of what it is intended to cover below, so the real risks do not become hidden over time).



CCTV for human rights organisation funded by Front Line

2.1.4 Agree the contents of the security plan – see (2) below for ideas. You will need to include security policies and procedures and contingency plans.

2.1.5 Pick one of the biggest risks. As a large group, **discuss, agree and document what will be in your plan to reduce your vulnerabilities and increase your capacities in relation**

to this risk. If you have time, consider more risks. (You could do this by splitting your group into smaller groups, to save time. Allocate one different risk per group. Ask each group to feed back to the full group to present their plan. Discuss each presentation and agree the final plan for those risks.)

2.1.6 **Allocate responsibility for producing a draft plan for each remaining risk** to those most suitable to draft them. Give a deadline for production. Meet again at that deadline to **discuss and agree the final plans for the remaining risks and the final version of the Organisational Security Plan**.

2.1.7 **Communicate the Organisational Security Plan to those who need to act upon it** – preferably all staff. Although you may circulate the document, it is best to present it face-to-face to allow everyone the chance to discuss the importance of security and the Organisational Security Plan.

2.1.8 Ensure that **one person is responsible for monitoring the implementation and review of the Organisational Security Plan**. It might be better if this is not the leader of the organisation who will have many other concerns.

2.1.9 The Organisational Security Plan is a **work in progress**. It should be adapted any time new tactics for your security arise. It should be reviewed when a new risk arises, or a threat is received, to check that your tactics are adequate to deal with the danger. It should also be reviewed after this new danger dissipates, to check that the Organisational Security Plan made sense in the situation and was followed. When the Organisational Security Plan is revised, the **version and the date should be clearly identified**, so it is clear which is the up-to-date Plan.

2.2 'Traffic Light' Security Settings

Some HRDs advocate also having a simple plan based on traffic lights.

If the situation is 'Green', then all is proceeding as normal and no special security precautions need be taken.

If the situation is 'Amber' then there is increased risk and a number of precautions need to be taken.
If the situation is 'Red' then this is the highest risk situation and the highest security measures need to be taken.

Each organisation would need to create its own Traffic Light Security Settings based on their own context, threats, vulnerabilities and capacities. But here is a short example:

Example: 'Traffic Light' Security Settings

"We talk to our donors in advance about financial assistance to improve our security, for medical and life insurance, and how our families will be supported if we are imprisoned or killed." HRD, Americas

The advantage of the Traffic Light Security Settings is that they are simple. They are easy to communicate to a large number of people and to communicate when the security setting changes. However, they are not a replacement for a fully thought through Organisational Security Plan and the development of awareness of security issues throughout the organisation.

Fig 5.1

Alert Level	Staff	Work Projects	Office
Green	• No restriction	• No restriction	• Normal security
Amber	• Staff most at risk (decided in advance) work at home • No staff to work alone in office or outside designated office hours • Reminder of who to ring in emergency • Alerted trusted neighbours / local community	• Sensitive projects put on hold (decided in advance which are sensitive) • Lawyer alerted • Other work continues	• Guard hired • No visitors allowed • Check no sensitive information available in office or homes • Alert trusted neighbours / local community • Alert police (if appropriate)
Red	• Staff most at risk relocate (which staff and where is decided in advance) • Other staff do not come to work	• All work halted temporarily • Advise donors	• Office locked • Additional guard hired

2.3 Contents of an Organisational Security Plan

Every organisation producing an Organisational Security Plan will do it differently, depending on their context, the risks they face, the threats they receive, their vulnerabilities and their capacities.

Overleaf are some headings which you may wish to consider for inclusion in your Organisational Security Plan.

"All our staff know what a search warrant looks like. They know how to check it. They know if the authorities come to search our office they do not have the power to search the people too. So if our office is to be searched, we hide our small laptops down our jeans."

HRD, Eastern Europe

Fig 5.2

Heading	Examples of Possible Content	Notes
Organisation's mission	Eg "We provide free legal assistance for people who can't afford lawyers"	This should be short and concise; staff should be able to repeat it quickly (eg at a road block)
Organisation's statement on security	• Staff may refuse assignments if they assess them as too dangerous (without disadvantaging themselves)	
General statement on security	• Security is not just about obeying procedures, but about always practising situational awareness and common sense • Security is for everyone – if one person neglects one area, it can put the whole organisation at risk	
Key roles and responsibilities	• Person who is overall responsible for security • Duties of other staff, including planning and evaluation, insurance, implementation. • Individual responsibilities: following rules and procedures; reducing risks, communicating security incidents, safety in personal life	Job titles are better than names – they tend not to change
Crisis Management Plan	• Definitions of types of emergency that brings this Plan into action • Roles and responsibilities, including: setting up a Crisis Committee, communicating with staff, with relatives, with authorities, with the media, with donors, etc.	For unanticipated emergencies
Security Policies and procedures	• Office security • Home security • Dealing with clients, witnesses etc • Computer and phone security • Information management and storage • Going on field trips • Vehicle maintenance and use • Avoiding attack (theft, assault, including sexual assault) • Dealing with cash • Dealing with the media • Dealing with the authorities • Stress reduction in the organisation	The contents will relate to your context. Some of the policies and procedures will overlap; repeating the procedures is better than complicated cross-referencing
Contingency Plans	• Detention / Arrest / abduction / death • Assault, including sexual assault • In the event of a coup	These are 'what to do if...' plans. The ones you need depend on your context and the risks you face.

Documentary made of HRD the Venerable Sovath Luon (right) helped raise profile and provide protection