CHAPTER 1.7

Preparing a security plan

Purpose:

Learning how to draft a security plan

Drafting a security plan

Now that you have drawn the map of stakeholders in protection, determined the field forces, assessed your risk, recognised your strategies already in place, and established your global strategy, it should not be difficult to draft a security plan.

Security is complex and the combination of several factors. Some must always be present. Others can be added when needed. Together they constitute the security plan.

They need to be implemented at an individual, organisational and inter-organisational level.

How to proceed? Here is a process in just a few steps:

1 ◆ **Components of the plan.** A security plan is aimed at reducing risk. It will therefore have at least three objectives, based on your risk assessment:

- Reducing the level of threat you are experiencing;
- Reducing your vulnerabilities;
- Improving your capacities.

A security plan should include day-to-day policies, measures and protocols for managing specific situations.

Day-to-day policy and measures for routine work

- Permanent advocacy, networking, codes of ethics, culture of security, security management, etc.
- Permanent measures, to ensure that routine work is done in accordance with security standards

Specific situation protocols:

- Preventive protocols: for example on how to prepare a press conference or a visit to a remote area
- Emergency protocols for reacting to specific problems, such as detention or disappearance.

The more day-to-day policies and measures that are implemented, the more the specific situation protocols will work.

Some examples:

- if a permanent set of policies and measures on information management is implemented, an office raid (emergency) will have less impact than where none existed

- if a permanent set of policies and measures on public relations is implemented, an early warning triggered by an attack against a HR defender will be more likely to elicit a reaction from key stakeholders, achieving the objective set by the defender in the event of an attack.

  To achieve the latter, the security plan will include permanent advocacy with duty-bearer and key stakeholders. It will need a permanent ethical behaviour policy operating in all aspects of the organisation's work, as well as the individual/organisational/inter-organisational levels.

- in the event of a detention, if a permanent plan is in place including policy on the ethical behaviour of individuals, then personal breaches of common law may reasonably be excluded as a cause and the emergency protocol can be implemented. Of course, common law infraction could be a pretext, but the organisation's lawyer or jurist will know what to do. Furthermore, the detained defender will know that steps are being taken and can recite them to themselves almost to the actual timeline and "relax" (psychological impact), knowing that outside action has started. There is no need to challenge the authorities and expose oneself to more risk than what s/he is already undergoing.

- in case of field missions into dangerous areas, relevant key stakeholders will have been previously informed and will be on standby until the team comes back safely.

2 ◆ **Responsibilities and resources for implementing the plan.** To ensure that the plan is implemented, security routines must be integrated into daily work activities:

- Include context assessment and security factors routinely into your schedule
- Register and analyse security incidents
- Allocate responsibilities
- Allocate resources, i.e. time and funds, for security.

3 ◆ **Drafting the plan - how to begin.** If you have done a risk assessment for a defender or organisation, you might have a long list of vulnerabilities, several kinds of threats and a number of capacities. You can't realistically cover everything at the same time. So where should you begin? It's very easy:

- **Select a few threats.** Prioritise the threats you have listed, be they actual or potential, using **one** of these criteria: the most serious threat - clear death threats, for example; **OR** the most probable and serious threat - if organisations similar to yours have been attacked, that is a clear potential threat against you; **OR** the threat which corresponds most to your vulnerabilities - because you are more at risk due to that specific threat.
- **List your relevant vulnerabilities.** These vulnerabilities should be addressed first, but remember that not all vulnerabilities correspond to all threats (see example below)
- **List your relevant capacities.**

Example

of selection process leading to the drawing up of a security plan:

The leader of a defenders' organisation (whether rural or urban) has received serious death threats. The organisation carries out the risk assessment of the threat and lists its vulnerabilities and capacities.

In conclusion, the organisation decides to implement the following security measures: secure all cupboards, fit iron bars to protect the office windows, purchase new cell phones for the members most at risk and publicly decry the death threats.

In general, the point is to ask and demonstrate how each measure is going to contribute to reducing the specific risk (in other words, how it is going to increase the security related to the specific risk)?

So: how are all these measures going to actually reduce the specific death threat against the leader? (Of course, they might address the global security of the organisation but this is not the right time to deal with it).

Ask yourself: What is the likelihood of the death threat being carried out at the office knowing that there are people around? Does the leader need to be at the office to be killed? The threatened leader will not always be at the office. So, there are other many other vulnerabilities, such as leaving the office alone late at night, or travelling to isolated areas, ignoring security measures whilst at home...

Although securing cupboards is important, it will not reduce the threat and vulnerabilities to the leader. The same goes for the iron bars on the windows. What could they do against a sniper and or a grenade?

How is a cell phone going to reduce that risk? (what can actually be done with a cell phone to prevent someone from killing the leader?)

It may be more useful to reduce the leader's exposure while commuting from home to the office or at weekends. These are the vulnerabilities that need to be addressed first as they are far more relevant to such a threat.

If the process selection is correct and you are in a position to address the selected threats, vulnerabilities and capacities in your security plan, you can be reasonably be sure that you will be able to reduce your risk from the right starting point.

Please note that this is an *ad hoc* way of drafting a security plan. There are more "formal" ways to do it, but this method is straightforward and makes sure you take care of the most urgent security issues - provided your risk assessment is correct - and end up with a "live" and "real" plan at the end: that is the important part of security. *(Please see the end of this Chapter for a detailed list of possible security plan components which you can also use when assessing your risks.)*

Possible items to include in a security plan

This "menu" details suggestions for factors to include in a security plan. After carrying out a risk assessment, you can pick and mix these ideas to complete your security plan.

A security plan includes elements that become political procedures (like meeting the authorities and international bodies, claiming the protection due from the state) and operational procedures (such as routine preparations for a field mission).

Elements of permanent policies and measures for the ordinary work:

- The organisation's mandate, mission and general objectives (knowing and respecting them).
- An organisational statement on security policy.
- Security should cut across all aspects of daily work: context assessment, risk assessment and incident analysis, as well as security evaluation.
- How to ensure that all organisation members are properly trained in security to the required level and that people's security responsibilities are passed on when they leave the organisation.
- Allocation of responsibilities: Who is expected to do what in which situation?
- How to handle a security crisis: Setting up a crisis committee or working group, delegating responsibility for handling the media, communicating with relatives, etc.
- Organisational security responsibilities: Planning, follow-up, insurance, civil responsibility, etc.
- Individual security responsibilities: continuing to reduce risk, how to handle free time or leisure activities, reporting and recording security incidents, sanctions (some of these points could be included in work contracts, where relevant).

- Organisational policies on:
  - rest, free time and stress management
  - the security of victims and witnesses
  - health and accident prevention
  - links with authorities, security forces and armed groups
  - information management and storage, handling confidential documents and information
  - your own image in relation to religious, social and cultural values
  - security management in offices and homes (including for visitors)
  - handling cash or valuables
  - communication means and protocols
  - vehicle maintenance
  - security of women defenders
  - security of LGBTI defenders
  - ...

Elements of specific measures for extraordinary work and situations

- Prevention and reaction protocols:
  - preparing field trips
  - landmines
  - reducing the risk of getting involved in common crime, armed incidents or sexual attacks
  - reducing the risk of accidents when travelling or in risky areas
  - reaction protocols on: medical and psychological emergencies (also in the field)
  - personal injury, attacks, including sexual attacks
  - robbery
  - when a person does not show up when they are supposed to
  - arrest or detention
  - abduction, disappearance
  - fire and other accidents
  - evacuation
  - natural disasters
  - legal or illegal searches or break-ins into offices or homes
  - if a person comes under fire
  - if someone is killed
  - in the event of a Coup d'État
  - ...

Implementing a security plan

Security plans are important, but they are not easy to implement. Implementation is much more than a technical process - it is an organisational process. This means looking for entry points and opportunities, as well as barriers and problems.

A security plan must be implemented on at least three levels:

1 ◆ The **individual** level. Each individual has to follow the plan in order for it to work.

2 ◆ The **organisational** level. The organisation as a whole has to follow the plan.

3 ◆ The **inter-organisational** level. Some level of cooperation between organisations is usually involved to maintain security.

Examples

of **entry points** and **opportunities** when implementing a security plan:

- Several minor security incidents have taken place in your own or another organisation and some staff members are worried about it.
- General security concerns exist because of the situation in the country.
- New staff arrives and can be trained to start good security practices more easily.
- Another organisation offers you security training.

Examples

of **problems** and **barriers** to implementing a security plan:

- Some people think more security measures will lead to an even greater workload.
- Others think the organisation already has good enough security.
- "We haven't got time for this stuff!"
- "OK, let's make extra time to discuss security on Saturday morning, but that's it!"
- "We need to take better care of the people we intend to help, not ourselves."

Ways of improving the implementation of a security plan

- **Take advantage of opportunities and entry points** to face problems and break through barriers.

- **Proceed step-by-step.** There's no point in pretending that everything can be done at once.

- **Emphasise the importance of security to core work on behalf of victims.** Stress that the security of witnesses and family members is critical to the effectiveness of core work and that this can best be managed by integrating good security practices into all areas of work. Use examples in training/discussion that demonstrate the potential negative impact of lax security on witnesses and victims.

- A plan drafted by two "experts" and presented to a whole organisation is likely to fall flat on its face. In security, **participation is key.**

- **A plan must be realistic and feasible.** A long list of things to do before every field trip will not work. Keep to the bare minimum necessary to ensure security. This is another reason to involve those who really do the work - for example, people who usually go on field trips.

- **The plan is not a one-off document** - it must be reviewed and updated all the time.

- **The plan must not be seen as "more work", but as "a better way to work".** People must be made to see the benefits, for example, by avoiding duplicate reporting. Make sure field trip reports have a security dimension, make security issues part of normal team meetings, integrate security aspects into other training, etc.

- **Emphasise that security is not a personal choice.** Individual decisions, attitudes and behaviour that impacts on security can have consequences for the security of witnesses, family members of victims and colleagues. There needs to be a collective commitment to implementing good security practices.

- **Time and resources must be allocated** to implementing the plan, as security cannot be improved by using people's free time. In order to be seen as "important", security activities must be placed alongside other "important" activities.

- **Everyone must be seen to follow the plan,** especially managers and those responsible for other people's work. There must be consequences for individuals who persistently refuse to abide by the plan.

Summary

A security plan has to decrease vulnerabilities and increase capacities so that threats are being reduced or made less feasible and therefore the risk is reduced.

A security plan must fit your actual needs and work space.

The point is not necessarily to cover a big socio-political space -rather to be within the right space and to cover as much of the working environment as possible, through networking and in conjunction with other organisations. Establish security procedures that transcend political differences.

Security is the concern of all and it is individual, organisational and inter-organisational.

Security is complex and is the result of several factors. Some must always be present. Others will be added at specific moments. Together they constitute the security plan.

Your security plan should include day-to-day policies, measures and specific situation protocols.

Both include political procedures and operational procedures.