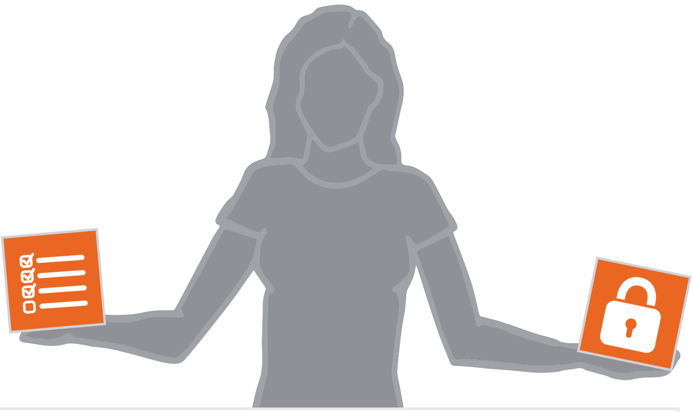
7. PREPARING A SECURITY PLAN



> **CHAPTER 1.7** OF THE NEW PROTECTION MANUAL
PREPARING A SECURITY PLAN

LEARNING OBJECTIVES

- Participants identify their own security and protection objectives.
- Design a security plan.

KEY MESSAGES

- A security plan helps to decrease vulnerabilities and increase capacities so that threats are addressed – or made less likely, thereby reducing risk. It is preferable to have a simple security plan that defenders will implement than a complex one that they probably will not.
- A good risk analysis leads to the identification of the main threats, vulnerabilities and capacities, in order to emphasise what is most important in the security plan. In case HRDs do not have much time or many resources, this will allow them to ensure that resources are allocated to priority security issues.

THE SESSION

CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Drafting a realistic and simple security plan, focusing on priority issues.
- Getting participants to accept the plan and indicating to them how to start implementing it in the short and medium term. Taking into account the specific protection needs that women HRDs and any other relevant social category of HRDs (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.) may have in terms of strategies, security norms, etc., both for routine protocols and emergency procedures.

THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
20´		**Introduction**: • Objectives and structure of the session • Objectives of security measures	Have the points ready on a flipchart (or PowerPoint slide)
90’	110’	**Drafting a security plan**	Results of risk analysis carried out in session 5.2 Flipcharts from session 5.2 Flipcharts Markers Table templates for designing a security plan (can be either projected from a laptop or prepared on flipcharts)
10’	120’	**Conclusion**	
		TIME KEEPING: CALCULATE 140´ (2 HOURS AND 20 MINUTES), INCLUDING A 20´ BREAK	

LEARNING ACTIVITIES

OBJECTIVE OF SECURITY MEASURES

To introduce this session, state the three general objectives that a security plan should contain:

→ Someone stops doing something, i.e. the aggressor does not threaten or attack HRDs.

→ Someone does what s/he has to do, i.e. the legitimate authority prevents aggressors from harming human rights defenders.

→ HRDs become less vulnerable and increase their protection capacity.

Use examples drawn from the participants’ own experience to illustrate these three objectives. Then remind participants of the risk equation (See NPM and Chapter 5.2. of this Guide). Point out that the first two objectives refer to threats and the last one to vulnerabilities and capacities. You should also stress the fact that the first two objectives are linked to their capacities. Indeed, the measures they take will increase their capacity to deter or dissuade potential aggressors.

DRAFTING A SECURITY PLAN

Developing a full security plan is a complex activity that requires considerable time. In this exercise, you will just focus on how to design a simple security plan based on the priorities established by an organisation’s risk analysis.

HOW TO WORK :

This work is based on the risk analysis carried out previously. When training a homogenous group, refer back to the results of the risk assessment exercise from Chapter 5.2. (see the Tips for Facilitators if working with mixed groups). Make sure you have the flipcharts from this exercise at hand to facilitate the process.

1. **Select the most specific threats:** Participants choose the most serious threats or the ones most closely related to their principal vulnerabilities, because they face greater risks from these threats (See NPM, Chapter 1.2 for hints and clues). (10 minutes)
2. **Re-assess vulnerabilities:** Give participants a few minutes to re-assess the vulnerabilities they have previously associated with selected threats. Make adjustments where you think this is necessary. You should focus in particular on these associated vulnerabilities when planning actions to reduce the risk that the selected threats will materialise. And remember, not all vulnerabilities are associated with every threat. (10 minutes)
3. **Re-assess capacities:** Ask participants to carry out the same exercise for the list of capacities they previously associated with the selected threats. (10 minutes)
4. **Turn vulnerabilities into "objectives" in the security plan:** see table below for guidance (the example does not claim to be exhaustive). (30 minutes)

Threat	Objective	Vulnerability (related to the threat)	Objective
"Break-in – other offices have been broken into".	"To reduce the possibility of a break-in at our office". "To reduce the negative impact of a break-in at our office should it occur".	"We have sensitive information stored on the office computers".	"Even if a break-in occurs we prevent: • the loss of information stored on the computers and; • unauthorised people from accessing that information".

5. **Develop each objective:** Write down actions that could be taken to achieve the objective. Draw the attention of participants to the fact that security measures should include preventive actions and reactive measures. Those objectives and actions will constitute an outline of the security plan (30 minutes). For example:

Objective	Actions
"To reduce the possibilities of a break-in at our office".	• Together with other organisations, issue a public statement denouncing the number of break-ins experienced by organisations, and demanding that the government put measures in place to stem them. • Put pressure on the relevant authorities (police and legal) to investigate the motives behind the break-in and who was responsible, and to bring them to justice.
"Even if a break-in occurs we will not lose the information stored in the computers and other people will not have access to that information". Note: This objective relies on organisations having the support, through networking, of external IT teams.	• To set up a computer network with a central server. • To regularly make backups/copies of the central server hard drive and keep the copy in a safe or protected place, external to the office. • To install a secure and simple encryption program for the central server, so that even if the hardware is stolen, the information stored in it cannot be used.

6. **List all actions to be taken in the form of a plan:** For this, project the table presented below onto a screen. Use the example provided or use one derived from the group's own experiences. Alternatively, write key elements on a flipchart to guide participants later on in their group work. Ask participants to form groups of 4-5 people and assign an equal set of selected threats to each group. Each group is to develop security measures for every threat that is assigned. To make this a realistic/operational plan, emphasise that it is important to give each action a deadline, and to assign responsibilities. Later, each group should present its results in the plenary, and the proposed actions should be discussed in plenary. At the end of the exercise, they will have the outline of their security plan.
The more time you have to spend on this exercise, the more concrete a plan can be produced, which the organisation can begin to work on immediately after the training.
The following table illustrates further elaboration of the plan using the same example:

Objectives					
Comprehensive (related to threats)	Specific (related to vulnerabilities)	Security measures	Responsibilities	Costs	Timetable
"To reduce the possibilities of a break-in at our office"	"Even if a break-in occurs we prevent: • loss of information stored on the computers and; • unauthorised people from accessing that information"	Classify which information is sensitive to take additional steps to protect from unauthorised access	**Programme officers and management**	**$0**	**Within 3 months**
		Build a computer network with one central server at the officer – the latter must not be easily accessible to outsiders	**IT officer/ external IT consultant**	**$0**	**Within 3 months**
		Buy external hard drive	**Finance officer**	**$200**	**Within 2 weeks**
		Make backups/copies of the central server hard drive once every week	**Information/ communications officer**	**$0**	**Every month**
		Keep a copy of the back up in a safe or safe place (external to the office).	**Programme Manager**	**$0**	**Every six months**
		Identify, learn how to use and use a simple encryption program	**Information/ communications officer**	**$0 (if using open software)**	**Within 2 months**

	Internal training on the encryption program & strong passwords	**All**	**$0**	**Within a month**
	Install encryption program for the central server and the backup, so that even if both are stolen, the stored information cannot be accessed	**Information/ communications officer**	**$0** (if using open software)	**Within 2 weeks**
	Together with other organisations, issue a public statement denouncing the number of break-ins experienced by organisations, and demanding that the government put in place measures to stem them	**Information/ communications officer**	**$0**	**Within a month**
	Put pressure on the relevant authorities (police and legal) to investigate the motives behind the break-in and who was responsible, and to bring them to justice.	**Advocacy Officer**	**$0**	**Immediate**

→ **Share the following insights with defenders about initiating the process of preparing a security plan:**

- **A security plan is only useful, if implemented:** Having a security plan does not automatically reduce risks. Plans need to be shared, explained and implemented to have an impact on the security of defenders.
- **Security management is a dynamic process that evolves, and requires regular evaluation:** Risks are dynamic, as they depend on an environment that is ever-changing; a good plan today may no longer be appropriate in six months' time. If the situation evolves, defenders should review their analysis and plan. Security management should be understood as a permanent process, based on the analysis of changing threats, vulnerabilities and capacities, as well as the socio-political context.
- **Security plans must be realistic if they are to be effective:** An effective security plan must take into account a realistic timeframe and the organisation's capacities. If the plan is too ambitious or demanding, it runs the risk of being shelved. Your role as facilitator is to ask questions that help defenders to assess whether their planned actions are realistic and achievable.
- **Security plans should encompass a reactive and a preventive dimension.**

→ **Difficulties when carrying out the activity on drafting a security plan:**

- You may be working with a large list of threats and vulnerabilities and this creates difficulties. Once you have selected the threats, only the vulnerabilities directly related to them should be selected. This will make the exercise easier. It will also allow the plan to target priority security issues. See NPM Chapter 1.7. for concrete examples.
- If you have a mixed group, you will need to make up an example or divide participants into groups

(each group corresponding to one organisation). An easy way would be to build on the activity conducted in **Chapter 5.2**. of this guide. Bear in mind that if there is a lack of trust between participants, it may be difficult to share details about risk analysis and about real security plans (hence the utility of working on fictitious examples). However, each organisation should do its homework so that it can define its own security plan following the workshop.

- Participants might mistake objectives for actions. This should not be a problem as long as they manage to define relevant and concrete security measures. So, do not waste too much time on conceptual clarifications. Your efforts should instead be focused on reaching concrete outcomes.

CONCLUSION

> Ask participants to recall the key learning points.

> Remind them of the importance of integrating the previous activities covered in the sessions on security management (context analysis, risk assessment, threat and security incidents analysis) into the design of the security plan.

> Remind participants that reading the relevant chapter of the NPM will be useful for the details of the work ahead.

ADDITIONAL RESOURCES

> Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).

> FLD. Op. Cit. Chapter 6.