4

Security in Groups and Organisations

There are a number of additional issues which arise when we approach security planning from within a structured group or organisation. Organisations develop their own hierarchies, cultures, strategies and means of planning into which the process of building security strategies and plans must 'fit'.

The process of planning for security in a group can be stressful for a number of reasons. It forces us to accept the genuine possibility of unpleasant things happening to us in the course of our work which can cause us or our friends and colleagues to become emotional or scared. It can also be difficult to consider all the possible variables and come to practical agreements about them.

Furthermore, in order to achieve organisational change successfully, we have to identify a process which can be both sufficiently inclusive and respectful of existing hierarchies where necessary. We must also recognise the personal nature of security and the need for the change to be managed in a way which encourages openness and recognises the distinct needs of different members of the group in accordance with not only the threats they face, but also aspects such as gender identity.

In this Chapter, we explore some of the key issues around building and improving security strategies and plans within organisations.

Creating and maintaining security plans

It's important to keep the following in mind when creating security plans following a risk analysis as explored in the previous segments, as part of a group or organisation.

Achieving buy-in

When introducing new people to existing plans in particular, it's important to go through some key points of the previous steps so that they understand how you arrived at the conclusion that these threats are plausible enough to plan for. Remember, as we explored in **Section I | Prepare**, security can be a very difficult issue to tackle as it is wrapped up not only in our physiological instincts, but also in our individual experiences of stress, tiredness and trauma. We

must remember to be patient and compassionate and work with our friends' and colleagues' perceptions rather than anything we consider (perhaps falsely) to be 'objective'. It's important not to scare people, but rather to try to create a relaxed and safe space in which people can express their questions and concerns and make commitments to act in a certain way during emergencies.

Participatory design

Some people will not react particularly well to having a security plan or agreement set without their consultation. High-risk activities and emergencies can be very distressing situations and it's important that each person is comfortable with the role and responsibilities they are assigned and has a space to express their concerns about this. In this regard, it's important that the process of security planning be as open and participatory as possible while still requiring a minimum commitment from all of those involved.

Role-playing

In some cases, it may be useful to design a role-play so that members of the organisation can practice how to respond to a certain emergency. Of course, this should be done carefully: avoid carrying out role-plays which may cause any team members to become distressed, especially those who have been victims of violations in the past. Be sure to get a sense of how organisation members feel about any role-play idea in advance and give them the opportunity to opt out if necessary.

Re-planning and considerations

Remember that all security plans should be live documents and processes. Once 'written' or agreed upon, they should not just be put in a drawer or on shared drive never to be read again! Rather, they should be re-evaluated and discussed regularly, especially when new members join the group in order to facilitate their acceptance and to allow new members to become familiar with them. Make it part of your security planning to include fixed dates to review your security practices and plans. It is also useful to include security issues in your strategic planning process to make sure security is not an afterthought. Doing this helps to ensure that security considerations are part of how you devise your strategy, develop activities, make necessary budget allocations and pro-actively address existing capacity gaps.

Emergency planning in groups and organisations

Like individual human rights defenders, groups and organisations ought to make emergency or contingency plans too in case our attempts to reduce the likelihood of an aggression or accident fail. When creating such plans in a group or organisation, here are a few key elements to keep in mind.

Definition of emergency

The first step in creating an emergency plan is to decide at what point we define a situation as an 'emergency' – i.e. the point at which we should begin to implement the actions and contingency measures we planned. Sometimes, this will be self-evident: for example, an emergency plan for the arrest of a friend or colleague would probably define the moment of arrest as the point at which an emergency should be declared. In other cases however, it may be less obvious: if a colleague carrying out a field mission stops answering their phone and can't be reached by other channels, how long should we wait before defining the situation as an emergency? These are agreements which, in the case of each threat, will have to be decided by you, your friends and your colleagues.

Roles and responsibilities

Depending on the number of people involved (be they your affinity group, collective, organisation, etc.), it is helpful if each person has clear roles that they are aware of and have agreed to in advance. This should help reduce disorganisation and panic in the event of an incident. In the case of each threat, consider the roles that you may have to assume and the practicalities involved in responding to an emergency.

In many cases, an important strategy for emergencies is the **activation of a support network**. A support network consists of a broad network of our allies, which may include our friends and family, community, local allies (e.g. other human rights organisations), friendly elements of the State, and national or international allies such as NGOs and allied journalists. Activating a support network, or some elements of it, during an emergency can greatly raise the cost of the aggression for those responsible and cause them to cease further attacks.

Return to your actor map (established in **Exercise 2.3 a/b**) and consider, for each threat scenario, the ways in which your allies may be able to support you. It may be useful to establish contact with them and verify that they will be willing to help you and know what you expect them to do in cases of emergency. In the case of State officials, it is good to consider this in terms of their position and perhaps

make reference to any local or international laws that would be useful in justifying this.

Channels of communication

Coordinating a response to an emergency always involves coordination of actions and often a lot of improvisation. In this regard, digital communication is increasingly important. It's important to establish what the most effective means of communicating with each actor is in different scenarios – and to identify a secondary means for back up too. Be aware that for emergencies, it might be useful to have clear guidelines on:

- what to communicate
- which channels to use (consider the sensitivity of the information, and the security of the channel: is it encrypted?)
- to whom?

Early alert and response system

An Early Alert and Response System is a useful tool for coordinating our response to an emergency – which may begin in the event of an accident or attack, or when there are very strong indicators that one is imminent. The Early Alert and Response System is essentially a centralised document (electronic or otherwise) which is opened in response to an emergency and includes:

- all the details about the security indicators and incidents which have occurred, with a clear time-line
- clear indicators to be achieved which will signify that the risk has once again decreased
- after-care actions which must be taken in order to protect those involved from further harm and help them to recover physically and emotionally. In some cases, it will be important to consult professionals to establish the best conduct – for example in case of traumatic events, physical or sexual violence, or accidents involving dangerous materials
- a clear description of actions which have been taken and will be taken in order to achieve these indicators, with a time-line.

The Early Alert and Response System provides useful documentation for subsequent analysis of what has happened and on how to improve our prevention tactics and responses to threats in the future.

Improving organisational security management

Beyond the creation of a strategy or series of individual security plans, organisations have to consider security management and its implementation by managers, staff and volunteers as a process of consistent re-evaluation. Organisations which implement the correct security measures perfectly at all times are rare and there will probably always be room for improvement. Bearing this in mind, it's a good idea to regularly evaluate the extent to which our security strategy and plans are not only consistent with the context in which we're operating (see **Section II | Explore**), but also that they are accepted and implemented by members of the organisation.

Assessment

While we'll often be aware that there is room for improvement in our implementation of security practices, it can sometimes be overwhelming to identify where to start, what to prioritise and who should be involved. It's useful to carry out an assessment of the current situation which will help us to identify in more detail the particular aspects of organisational security management which we need to improve.

This assessment and subsequent process of improvement will need to be managed, coordinated and carried out by people either internal or external to the organisation. Internal staff who could be involved may include:

- the board of directors and executive directors
- management or senior staff
- regular staff and volunteers.

External entities who could be involved in the process would include:

- donors
- external consultants and trainers.

Involving each of these actors in the process has its own distinct advantages and disadvantages.[18] However, bearing in mind the personal nature of security, it is important that from the outset, the process is carried out in an inclusive,

18 For more detail on this see Chapter 1.3 "Managing organisational shift towards an improved security policy" in the New Protection Manual for Human Rights Defenders (2009) Protection International.

participative, transparent and non-judgemental manner. Formal hierarchies within organisations can often become a 'sticking point' when it comes to managing a sensitive and personal process such as this; it is important that management remains sensitive and aware of the needs of their programme and 'field' staff or volunteers, who are often those putting themselves at higher risk and/or benefiting less financially from their activism. Staff and volunteers should also respect the fact that management face a difficult task of standardising an approach to security and are doing so, hopefully, in the best interests of all.

Criteria for assessment

As mentioned, a logical first step in improving organisational attitudes, knowledge and skills regarding security is to carry out an audit of the current situation in order to identify the priorities for improvement.

In assessing how the organisation's security protocols are observed and implemented by management, staff and volunteers, it is important to look at some concrete issues and indicators, in order to avoid becoming overwhelmed. It may be useful to consider the following points:[19]

Acquired security experience

How much experience of implementing security practices exists among members of the organisation? Is this experience spread evenly across staff, or concentrated among a few individuals?

Attitudes and awareness

Are people aware of the importance of security and protection? Is their attitude towards it generally positive? Are they willing to continue improving? What are the barriers they perceive to this? Consider whether this fluctuates between attitudes and awareness regarding digital security, physical security and psycho-social well-being.

Skills, knowledge and training

As previously mentioned, in order to build new knowledge and skills, resources, time and space need to be made available for training (either formal or informal). Is such training available to members of the organisation? Does this include trainings on psycho-social well-being and digital security?

---

19 Based on Chapter 2.1 "Assessing organisational security performance: the security wheel" in the New Protection Manual for Human Rights Defenders (2009) Protection international.

Security planning	To what extent is security planning integrated into our work? How often are context analyses (see **Section I | Prepare**) carried out and security plans created? Are plans updated regularly, and do they include digital device management and stress management?
Assignment of responsibilities	Is there a clear division of responsibilities for implementation of our security practices? To what extent are these responsibilities observed, and what are the potential blockages?
Ownership and compliance	To what extent are organisation members involved in the organisational security planning, and to what extent do they observe the plans that exist? What are the problems which arise here, and how can they be overcome? How can the process be made more participative?
Response to indicators	How often are security indicators shared and how often are they analysed and subsequently acted upon if necessary
Regular evaluation	How often are the security strategies and plans updated? Is there a concrete process in place for this, or is it ad hoc? How can it be made more regular, what other problems exist and how can they be overcome? In the exercise below, you can explore some concrete questions to help establish the extent to which security plans are observed within your organisation.

3.4 Exercise

Assessment of organisational security performance

Purpose & Output	This is a basic exercise which checks perceptions of members of the organisation regarding the implementation of organisational security measures
Input & Materials	Some drawing materials or a copy of the security wheel exercise (**Appendix E**)
Format & Steps	You may want to focus on overall organisational security performance, or one more specific aspect of your organisation's security practices such as digital security, psycho-social well-being, travel security, security in conflict zones, etc. **Step 1:** Use the organisational 'security wheel' (**Appendix E**) or draw a circle and divide it into eight sections, each with a title (as in the diagram) to create your own security wheel. **Step 2:** For each segment of the wheel, colour in a proportion which, in your opinion, reflects the extent to which your organisation implements best practices. **Step 3:** For each segment, each person should identify the barriers which are currently preventing them or the organisation in general from better observing best practices **Step 4:** Similarly, consider what the potential solutions are for each barrier or problem. **Step 5:** Compare results among members of the organisations. Where is there consensus, and where are there differences? Why might that be? **Step 6:** Together, try to identify areas which must be prioritised for improvement.

Prioritising areas for improvement

Once an assessment of the current situation has been carried out, we should have an idea as to which areas should be prioritised for improvement. A plan for improvement should be drawn up on this basis, and disseminated among the staff and management. The plan should:

- have a clear objective in terms of new best practices to be implemented
- a time-line, including who needs to be involved in the process and what is expected of them
- clearly stipulate the resources needed for the improvement to be made.

Management should ensure that staff and volunteers are granted the time to undergo any required training or other capacity building necessary in order for this improvement to take place.

Overcoming resistance to security planning[20]

It is often the case that, within organisations, there is resistance among some management, staff, or volunteers to the security protocols they are expected to observe. There can be a large number of reasons for this.

When attempting to deal with resistance to security planning within the organisation, it's important to keep in mind that, as we have explored previously, security is a deeply personal concept. As such, people may have particularly personal reasons for resisting certain protocols which imply changes in their personal lives, their free time, or their relationships; they may also imply having to learn new skills which are challenging and taxing on their energies which may already be under stress.

The best approach to dealing with resistance to changes in security practices, therefore, is to create a safe space in which individuals can comfortably voice their concerns around it. As noted in **Section I | Prepare**, it is a good idea to practice active listening and non-violent communication in order to facilitate an open and constructive debate.

Below are some common resistance stereotypes, the reasoning underlying the resistance and possible responses to help defenders overcome resistance within their groups, organisations, or communities. Seeking to create space for discuss-

20 Based on material from Chapter 2.3, New Protection Manual for Human Rights Defenders (2009) Protection International, p.153.

ing security within a group where everyone's opinion and experience is respected and heard is key. Being aware of personalities, power dynamics and hierarchies is important when deciding on responses to overcome resistance.

Common Resistance Stereotypes

"We're not being threatened" or
"Our work is not as exposed or contentious as other organisations' work."

Reasoning behind the stereotype

The risk stays the same, it doesn't change or depend on the fact that the work context might deteriorate or that the scenario might change.

Responses to overcome resistance

Risk depends on the politicalcontext. As the political context is dynamic, so is the risk.

"The risk is inherent in our work as defenders" and
"We are already aware of what we are exposed to."

Reasoning behind the stereotype

The defenders accept the risk and it does not affect them in their work. Or, therisk cannot be reduced, the risk is there and that's all there is to it.

Responses to overcome resistance

- Meeting with inherent risk does not mean accepting the risk.
- The risk has at least a psychological impact on our work: at the very least it induces stress which affects the work and possibly the personal well-being of the defender and the group.
- Risks faced by defenders are made up of various elements – threats as the external force seeking to impede or stop their work, defenders' vulnerabilities and capacities in relation to the threat(s): vulnerabilities and capacities as variables that a defender can influence. By identifying and analysing threats and their risk, defenders are able to realise existing vulnerabilities and capacities/strengths and undertake targeted efforts to reduce their vulnerabilities and increasing capacities. This will reduce the risk even if it is not entirely eliminated. Creating space in an organisation to analyse risks and jointly agree on

strategies to reduce them can have an empowering effect on individuals and the group, increasing the individual and collective sense of security to continue their work.

"We already know how to handle the risk", or
"We know how to look after ourselves" and "We have a lot of experience."

Reasoning behind the stereotype

The current security management cannot be improved and it is therefore not worth doing. The fact that we have not suffered harm in the past guarantees that we won't in the future.

Responses to overcome resistance

- Security management is based on the understanding that risks faced by human rights defenders result from the political environment and the impact their work has on different actors' interests. Because this context is dynamic, risk is also dynamic, requiring constant analysis and adaptation of strategies. In addition, stakeholders change their position and strategies, also necessitating adaptation by human rights defenders to manage risks.
- Experience in advancing human rights and defending the rights of others requires you to constantly evaluate your strategy, create space for your work, identify support. This is the same when managing your security. If you want to have an impact with your work and protect the people you work for and with, you need to stay well and safe. And at the same time there is a somewhat moral obligation for you to not put the people you work with at further risk.

"Yes, the issue is interesting, but there are other priorities."

Reasoning behind the stereotype

There are more important issues than security of defenders.

Responses to overcome resistance

- First and foremost, defenders are people. They have families, friends, communities who need them and whom they need. Self care is a political act. Defenders' adversaries aim to cause harm, fear, anxiety and/or stress to hinder or stop their work. Being alive and well is a prerequisite to continuing a struggle against injustices.

"And how are we going to pay for it?"

Reasoning behind the stereotype

Security is expensive and cannot be included in fundraising proposals.

Responses to overcome resistance

- Thinking of one's security is not a weakness, it is a strength that will ultimately benefit the people you work with and for.
- Security is a very individual concept. In many cases it is closely related to defenders' attitudes and behaviours. Improving one's security often requires a change in attitude and subsequent change in behaviour and practices that often don't cost anything at all - at least not in monetary terms.
- Donors and partners are interested in a continuation of defenders' work. They will prefer to work with an organisation which recognises security issues instead of running the risk of an end to their work and a potential loss of their investments.

"If we pay so much attention to security we won't be able to do what is really important which is working with people and we owe it to them."

Reasoning behind the stereotype

Our own security and well-being does not impact our ability to help others. Our security and well-being are irrelevant to those we work with and for.

Responses to overcome resistance

- Security is a very individual concept and requires every individual to make decisions of the risks acceptable to them. Being sensitive to our security is part of our resistance against those who want to harm us for the legitimate work we do. We are much less able to take care of others if we do not take care of ourselves.
- If we care for ourselves and our security, we will be better prepared to care for those around us.
- People run risks by entrusting us with their cases and if we do not work on our security, it will affect them too; they might choose to trust another organisation that has adequately planned its security and is thus also giving more security to other people.

"We don't have time as we are already overloaded."

Reasoning behind the stereotype

It is impossible to find time in the work schedule.

Responses to overcome resistance

- It's a false distinction to think about security and well-being 'versus' our work. Security and well-being will make our work more sustainable. It is strategically more effective in the long term to make this space.
- Security management does not have to take much time. It's often just about small changes in our day-to-day work.
- In the long run, we will save time responding to emergencies if we are prepared in advance, and moreover, will have to deal less often with the physical, emotional and economic consequences of emergencies that affect us as human beings and organisations.

"The community is behind us: who would ever (dare) hurt us?"

Reasoning behind the stereotype

We are part of the community. The community is not fragmented, does not change either in members and opinions. The community cannot be influenced.

Responses to overcome resistance

- The community is not homogeneous and is also made up of those who might be negatively affected by our work.
- Under pressure, sometimes even those who want to support us can turn against us.

"In our village, the authorities have shown understanding and collaboration."

Reasoning behind the stereotype

Local authorities are not affected by our human rights work and will not change their minds. There is no hierarchy between national and local authorities.

Responses to overcome resistance

- Organisational historical memory will have examples of local authorities opposing human rights work when their tolerance limits have been exceeded.
- Local authorities have to implement orders from above. Authorities are made of people who might have an interest in protecting aggressors.
- Political contexts change.