5

Communicating about Security within Teams and Organisations

Once we understand how individuals and teams react to stress and threats, it becomes important to reflect on how healthy practices towards this can be fostered in our groups and organisations.

Creating a safe and regular environment for communicating about security within teams and organisations is one of the most important preparatory steps towards a successful security strategy and organisational well-being. All of the tools outlined in this and other resources which help us build our security demand time and space to be made for speaking, exchanging, reflecting and learning about security. Aside from this clear practical necessity, creating space to talk about security with our peers and colleagues helps us to:

- more accurately perceive the threats to our work (reduce unrecognised threats and unfounded fears)
- understand why members of the team might react differently to stress or threats (individual responses to threats)
- assign roles and responsibilities for security measures
- increase group ownership of security measures
- build solidarity and care for colleagues who are suffering from threats.

However, there may be barriers that prevent us from discussing security openly within our organisation. Some barriers may include:

- heavy workloads and lack of time
- simply being afraid to discuss it
- a sense that our observations on security might be perceived as fear, paranoia or weakness
- not wanting to confront colleagues about their practices
- not wanting to be the first to bring the matter up for discussion
- gender issues and/or power dynamics.

In order to create a space for discussion, we can engage in the following:

a. building trust within the team

b. regularly scheduling talks about security

c. fostering a healthy culture of interpersonal communication.

As we explore each of these, we will discuss ways to establish them, and some of the benefits (as well as the disadvantages) associated with each of them.

a Building trust within the team

Having a team that operates based on trust is optimal for productivity as well as for security purposes. Trust facilitates the implementation of new security measures, especially among members who could not be, or were not involved in making the decisions about it. It creates an atmosphere of openness in which members will more readily share their security incidents and the information they feel is important, and even their mistakes. It gives members confidence to know whom to talk to about which aspects of security.

There are several ways we can work on increasing trust within a team. Below are some examples of activities to accomplish this:

- Getting to know each other outside the professional or activist context, e.g. through out-of-work activities, socialising and having fun.
- Checking regularly on the well-being of team members (perhaps as a start to team meetings), to have an idea about everybody's stress levels, general mood and what they are bringing to their activism from their personal lives.
- Transparency about hierarchies and decision-making structures.
- Clear protocols for how to deal with personal or sensitive issues that may arise including (but not limited to) security incidents, threats and so on.
- Having access to a counsellor or trusted psychologist.

Building trust within a team is not a trivial task – it involves investment and taking risks, given the potential for infiltration noted above. However, in this regard, aside from trust in one another, we can also build trust in our strategies for managing sensitive information, clear channels and create means for communication about it.

An atmosphere of trust also relies on everyone being able to give and receive constructive criticism and feedback, which will be explored in the segment on interpersonal communication below.

b Encouraging regularly scheduled talks about security

As explored in **Chapter 1.4 Team and Peer Responses to Threat**, it is essential to create regular, safe spaces to talk about the different aspects of security. When a team sets regularly scheduled time aside to talk about security, it elevates the

importance of the topic and the conversation. This way, if team members have concerns around security, they will be less anxious about seeming paranoid or wasteful of other people's time.

Scheduling regular talks about security also normalises the frequency of interaction and reflection on matters relating to security, so that the issues are not forgotten, and team members are more likely to bring at least a passive awareness of security to their ongoing work.

It is also important to incorporate security elements into the normal functioning of the group. As such, we avoid making security an extraneous element, but rather an integral part of our strategy and operations. For example, this can be achieved by adding security to the agenda of a regular meeting. Another way is to rotate the responsibility for organising and facilitating a discussion on security between members the group, so as to instil the notion that security is everyone's responsibility and not just that of a select few.

In situations of high risk, it is important to increase the number of check-ins at meetings and informal spaces, as well as raising group members' overall receptiveness to talking about security in a supportive atmosphere.

In the next exercise, you will find some questions to help you explore the culture within your group in regard to talking about security, identifying barriers and considering ways to deal with them.

1.5a Exercise

Talking about security in groups and teams

Purpose & Output	The purpose of this exercise is to reflect on how and when we talk about security with our peers, colleagues or team. It is best facilitated by at least two people, but can also serve as a useful individual reflection on your interaction with your colleagues. This helps start a process to constructively talking and discussing security in your team/group.
Input & Materials	To do this exercise in a participative way and in order to document it, you may need writing material (cards or stickies and markers). A large area of wall-space, a flip-chart or pin-board may also be useful.

Format & Steps

Individual work & group discussion

Step 1: Divide the group into pairs. Ask each pair to consider the following questions concerning group dynamics and write down their answers.

- What topics take up the majority of time in group conversations?
- What topics do we never seem to find time for?
- What aspects of our group interaction do we find energising?
- What aspects of our group interaction do we find exhausting?
- What happens in the group when people disagree?
- Have you created any space to develop and refine your own security practices (as an individual)? Describe it: where and when does this space exist? Is it sufficient, and how might you expand this space, if necessary?
- Do you have enough space to talk about security issues with others, such as peers or colleagues who work closely with you, and how might this space be created or expanded if necessary?

Step 2: Collate the full set of responses to these questions on a board or in a notebook.

Step 3: As a team, consider the following questions.

- Where and how do we want to set our priorities concerning security?
- What are common problems that arise around talking about security as a group?
- What can prevent us from talking about security? How can we deal with this?
- How can we create and maintain sufficient and adequate space for talking about security? What will this mean in terms of time and resources?
- How might we increase the effectiveness of our group interaction on security?
- What problems arise around committing to changing our security practices? Do we resist change, individually or collectively, and why?

Format & Steps

Step 4: Invite each person individually to reflect on:

- Whether you should have a similar awareness for your family and loved ones?
- What are the differences in the dynamics and ways in which family and loved ones are affected?
- In what ways do you communicate the threats you are facing to your family, community, friends and others not in your work circle?

Step 5: In the whole group, share the points that people feel free to share. Then you should agree on what can be communicated to those 'outside' the group, for reasons of confidentiality, intimacy and security. Agree on these guidelines for the whole group.

Remarks & Tips

Consider also discussing the steps and requirements necessary to put your ideas of how to talk about security in the future into practice.

Important questions to consider might be:

- What happens if you don't progress on 'talking about security'?
- What happens if someone does not stick to the guidelines on what can be communicated to the outside?

C Fostering a healthy culture of interpersonal communication

Individuals' ability and willingness to engage in open communication with each other is fundamental to creating a space where security can be frankly and effectively discussed.

We must make sure that communication among team members stays healthy and open, so that we have access to as much information as possible and can make more informed decisions, as a group, about our security.

Talking about security can, however, be challenging for a number of reasons, due to its very personal nature and the fact that our vulnerabilities and even mistakes are often very relevant information. Finding a constructive way to talk about security in groups or organisations helps avoid misinterpretations that can lead to conflict between the people involved.

Below are some aspects worthy of consideration in creating a healthy culture of communication:

Prevailing atmosphere around security

It helps to come to terms with what the existing (organisational) mindset around security is. For instance, we can reflect on whether the time allocated to talking about security is as valued and tended as other meeting times; or we can pay attention to whether group members are dismissive in voice and tone when discussing security matters; or if we are genuinely interested and personally connected when our colleagues are addressing their concerns.

Existing hierarchies

It is also important to create mechanisms for such communication across hierarchies within an organisation, so that members are able to discuss things in an atmosphere free of power dynamics.

Communication under stress

Paying attention to our communication style within teams becomes particularly important during times of increased stress. In times of threat and stress, we tend not to focus on our language and tone due to other extenuating circumstances. We may not even be aware of our impatience, or we may expect others to understand the reason behind our change in behaviour.

Intercultural situations

We also have to bear in mind that communication is a fundamental aspect of culture and cultural diversity. We should pay attention to our verbal and non-verbal communication in intercultural situations.

Formal modes of communication

Some groups tend to be more formal in communication and about decision-making in meetings. While formally establishing practices for security and well-being is useful in many contexts, this mode of communication can occasionally hinder open sharing, especially regarding the emotional aspects of security. Thinking about facilitation and formats for these discussions may help arrive at an effective structure that provides space for open sharing of hopes and fears, as well as for more technical discussions. It is important to incorporate all of these aspects when making decisions about security.

One example of a useful practice in interpersonal communication is through the method of **non-violent communication**. Non-violent communication is a method of communicating based on the assumption that all people are compassionate by nature, that we all share the same basic human needs and that each of our actions is a strategy to meet one or more of these needs.

While this method is certainly culturally shaped in the 'West', it allows for communication to include ways of comfortably reflecting on how the communication is affecting everyone involved. This can be especially effective for giving and receiving feedback about security and in discussing the impact of attacks, accidents, threats or other security-related events on us as individuals and groups.

A major advantage of employing such a particular way of structuring conversations and feedback is that it helps avoid accusatory manners of expressing views and encourages clarification where there is misunderstanding. In the following exercise, you can practice following the steps for giving constructive feedback on security according to the basic principles of non-violent communication.

1.5b Exercise

Non-violent feedback

Purpose & Output

The purpose of this exercise is to practice non-violent communication as a means of improving the effectiveness of communication about security within teams and groups. It provides for a reflection on how we can give our feedback in an understandable, clear way and avoid some of the pitfalls which can lead to arguments or ineffective communication.
The exercise is best carried out in pairs at first, although it can be adapted for larger groups.

Input & Materials

It may be useful to write the guidelines for non-violent feedback somewhere visible, like on a flip-chart.

Format & Steps

Decide on a setting for conducting a feedback discussion (this can be done in pairs, or with observers, taking turns). The participants should choose a topic (real or imaginary) about which they want

to give feedback. This can be a security-related topic, such as an incident which took place already, or something else entirely.
Ask the person giving feedback to follow the guidelines below. For each guideline, a small illustrative example is given. Here, we are imagining a scenario in which two colleagues are talking: one of the colleagues often works late and once forgot to lock the door of the office when leaving; the other colleague wants to talk about the incident.
The recipient of the feedback should only ask questions of clarification but not comment, reply, justify or question the content of the feedback.

Guidelines for non-violent feedback:

I speak for myself: You can only speak from your own subjective experience – not about 'common sense', 'my group', 'we', or 'one', but only 'I'.

- e.g. "I felt unsafe when I found the office unlocked this morning".
- Bad practice: "What you did yesterday put us in danger!"

What did you observe? You should speak only of the facts as you experienced them, so the interlocutor knows what your feedback is referring to (what you saw, heard, etc.).

- e.g. "When I arrived at the office this morning, the front door was unlocked and I could open it without the key".
- Bad practice: "You forgot to lock the door yesterday!".

What was your reaction to it? What were your internal feelings and physical reaction to your experience? Try not to be judgemental, but again, simply speak from your experience as you understand it.

- e.g. "I was very worried, because I thought maybe we had been robbed. When I found that everything was OK, I was still quite angry."

How do you interpret it? What does your personal interpretation bring to the facts? Although your personal interpretation is indeed subjective, it is still valuable and colours your experience.

- e.g. "I think it happened because you have been working very late and were tired and simply forgot to close it"

Format & Steps

What are your wishes, advice, or interests? What are your suggestions for change based on this experience? They should be offered without demands, but rather as requests for consideration by the group.

- e.g. "I would feel better if I knew we were all getting enough rest and not overworking so that we could better take care of things like this, so it would be better if you didn't work so late".

Ask the pairs to then share their insights on the process and manner of giving feedback – not about the content. Did they experience different feelings than when they normally receive feedback?

This exercise can also be used to clarify the content and tone of your feedback as a preparation for an actual feedback session or potentially difficult discussion.

Remarks & Tips

It is important to receive feedback with your ears and not with your mouth, and understand it as a personal reflection from your partner, not as 'the truth' or an invitation to justify or defend your actions. You decide yourself if it is valuable to you and how to react to it. Following such an approach might be a preventive step for conflicts within your team. As such, it can contribute to your overall well-being.

If you are interested in deepening modes of communication which deal sensitively with conflict, you might want to have a look at non-violent communication approaches.

Be aware that 'speaking for myself only' is not appropriate in many regions around the world. Adapt the methodology so that it fits your needs and setting.

Conclusion

Hopefully, these exercises will have helped you get a better sense of what security means to you, as well as a better understanding of the way you and those around you respond to threats to yourselves and your work. Establishing a healthy culture of communication as explored above may represent one of the more difficult changes to make in adopting a more positive and organised approach to our security and well-being. However, understanding this and all of the topics covered in this Section is vital in order to make space for the process of context analysis, a key set of activities in improving and maintaining an organised approach to security, which we will expand in **Section II | Explore**.