III Strategise

Responding to Threats with Strategies, Plans and Agreements

Contents

Introduction

In this Section, we will explore the process of developing and refining our security strategies, plans and tactics based on the threats identified in our context analysis. In order to do this, we must begin with the threats to ourselves, our work and our well-being that we identified in **Section II | Explore**. We will examine these threats in light of our current security practices, our capacities and vulnerabilities in order to establish the gaps that remain in our ability to properly respond to them.

Once we have completed a realistic assessment of our security situation, we can consider building new security strategies and formalising them into plans and agreements for different aspects of our work.

Alongside this process, we will consider some of the particular dynamics that arise for those of us who are trying to carry out security planning as an organisation, including assessments of organisational security practices, and engaging with the Do No Harm principle in security planning.

In Strategise, we will:

- examine our **capacities and vulnerabilities** relative to the threats we have identified
- identify **new** capacities we want to build and explore some key issues around security **capacity building**
- look at key elements for inclusion in **security plans** and the process of designing them
- explore key issues around security planning in larger **groups and organisations**
- engage with the **Do-No-Harm** principle and how it can be applied to our security practices.

1

Analysing our Responses to Threats

We will begin by analysing our existing security practices and responses to the threats we consider priorities. When it comes to security planning, very few of us will find ourselves starting 'from scratch': as mentioned before, we have certain instincts which help us to avoid or respond to threats in our daily life. Beyond that, we likely have certain socialised practices – often referred to as 'common sense' – which we unthinkingly practice in order to stay out of harm's way.

In this Section we are going to cast both an appreciative and critical eye upon these existing practices and identify steps we ought to take in order to develop security strategies, plans and tactics which correspond to the analysis we undertook in **Section II | Explore**.

Overall framework: Threats, capacities and vulnerabilities

In this process, it is useful to work with the concepts of capacities and vulnerabilities relative to each particular threat we identify.

- Capacities are the factors which help to keep us safer from a particular threat (i.e. reduce its likelihood or its impact).

- Vulnerabilities are the factors which make us more susceptible to a threat (i.e. they increase its likelihood or its impact).

Capacities and vulnerabilities may be characteristics of our own, our allies, or the environment in which we are operating which we consider relevant to our security.

Once we have identified our capacities and vulnerabilities as they relate to each threat we face, we can work on reducing our vulnerabilities and building our capacities in order to reduce the likelihood or impact of the threats: building capacities and reducing vulnerabilities help reduce the risk posed by a given threat.

Our existing practices and capacities

Using the threat analysis we carried out at the end of the last Section as a starting point, we will begin by analysing these threats in terms of our existing security practices and other capacities we can identify. Then, we can try to identify the gaps or vulnerabilities in our practices with a view to improving them.

We have already considered some of these existing practices for well-being and security generally in the previous Chapters but we'll now examine them in light of the threats we have identified. Even though this might be the first time that you have conducted a critical analysis of your security, some of your existing security and well-being practices may already be effective in preventing your high-priority threats from taking place. Security doesn't have to be complicated: it can include simple actions like locking the door to your office, having strong passwords for your online accounts or keeping a first-aid kit in your home.

However, it is important to avoid creating a false sense of security. We should think critically about our existing practices and whether or not they are truly effective in our context. The question is: how (if at all) do our existing practices relate to the threats we've identified?

In **Section II | Explore**, we considered our priority threats in great detail. We thought about:

- what the effects of each particular threat would be (if it came to pass)
- who may be responsible for the threat
- who or what would be the target of the threat
- how the threat would be carried out

- what information our adversaries would require for this
- where the potential attack would take place, and
- how our own mental and physical state may make us stronger, more resilient or conversely more susceptible and vulnerable to the threat.

In the next exercise, we will consider these questions in terms of our existing good practices.

3.1a

Exercise

Existing practices and capacities

Purpose & Output

In this exercise, you can consider each of the threats you already identified and prioritised in light of your existing security practices and other capacities relative to them.
This will give you a 'baseline' on which you can later build and improve.

Input & Materials

To carry out this exercise, you need to have identified and prioritised threats in **Exercise 2.6b/c**.
It may be helpful to write out the the capacities you identify so you can review them later.

Format & Steps

Return to the threats identified in **Exercise 2.6b**. For each of the threats you have identified, there were a series of questions. Here you can relate your existing security practices and capacities to each of these questions as follows:

- **Who/what** is under threat? Identify here what capacities (if any) are already protecting this person or thing from this threat. Examples of capacities could include
  - in the case of judicial harassment: good legal knowledge
  - in the case of computer confiscation: having encrypted hard drives.
- **Who** is behind the threat? Do you already have some kind of tactic for engaging with this actor? Are there any tactics or

Format & Steps

resources you have leveraged in order to prevent them from acting against you? If so, what? If they have acted against you before, did you respond in some way? If so, how? If you don't have any, that is fine: this will be important to remember when you identify gaps.

- **How:** What information is necessary for them to carry out the attack? Do you have any information protection or counter-surveillance practices in place which might prevent that information from falling into their hands?
- **Where:** What access to you or your property do they need? How do you secure the physical spaces around you (e.g. buildings, vehicles, private property) in order to protect yourself and your property? For example, do you lock your offices and homes? What 'common sense' practices do you have for your personal safety in dangerous environments? All of these are important to note, so that you don't start from zero!
- **Psychological, emotional and health tactics:** Include any well-being practices that are in place to deal with this threat – do you have any practices which help to reduce stress, tiredness etc., and increase centredness and awareness which may help respond to this threat?

Where possible, try to consider these aspects relative to each of the threats you have identified. **If you can't think of an answer for one or more of the questions, that is fine:** you have just identified a gap to be filled! You will consider gaps in the following exercise, and use them as a way to identify what new resources and practices you need.

Remarks & Tips

Caution! For each of the answers you give, consider **whether this practice or capacity is positive. How do you know?** There is a slight danger of creating a false sense of security if you falsely credit an existing practice with helping to keep you safe. If you are not sure about something, it would be worth taking the time to think over and **talk to your colleagues or trusted friends** in order to get a fresh perspective.

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	**Target**	**Adversary**	**How**	**Where**
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Identifying gaps and vulnerabilities

Now that we have identified our good practices and how they may relate to the threats we have prioritised, we should ask ourselves a slightly more difficult question: **What gaps remain** that may make us more vulnerable to these threats? What unhelpful attitudes or lack of sufficient knowledge or skills on our part represent vulnerabilities?

In navigating this question, it is important to remember that stress, tiredness and fear (among other factors) might inspire **unfounded fears**. Additionally, our resource limitations (or the sophistication of our adversary) may result either in inaccuracies when gauging the threats we recognise or in **unrecognised threats**.

Recognising such uncertainty where it exists is a positive first step which can propel us to **further investigate** the threats around us. We can also take steps to

check our perceptions by engaging in conversation as a group or with our trusted allies, colleagues and friends.

With that in mind, it is helpful to now return to your threat analysis and reflect on what details you know about the threats you face and your existing practices for preventing or reacting to them. Where are the gaps and vulnerabilities in relation to each of the aspects you considered?

3.1b Exercise

Vulnerabilities and gaps in our existing practices

Purpose & Output

In this exercise, you can consider each of the threats you identified and prioritised in **Section II | Explore**, in light of the gaps in your existing security practices and your vulnerabilities. This will give a much clearer picture of where you need to begin building new capacities.

Input & Materials

To carry out this exercise, you need to a) have identified and prioritised threats in **Exercise 2.6b**, and b) collated the output from **Exercise 3.1a** above.
Use pens and paper or other writing materials.

Format & Steps

Return to the threats identified in **Exercise 2.6b** and the existing capacities and practices you identified in **Exercise 3.1a**.
Here, you can attempt to identify the gaps in your existing practices and your vulnerabilities, relative to each of the questions you answered previously. Consider the following questions:

- **Who/what** is under threat? Identify here what gaps or vulnerabilities (if any) are making this person or thing more vulnerable to the threat. Vulnerabilities could include:
  - in the case of judicial harassment, a person having little legal knowledge, or
  - in the case of computer confiscation, the hard-drives having no password or disk encryption.

- **Who** is behind the threat? What vulnerabilities or gaps exist in our ability to influence this actor? For example, if there is no way of directly engaging with the actor to create acceptance of your work or deter an attack, this could be considered a gap.
- **How**: What information is necessary for them to carry out the attack? Is it difficult to control the flow of information – are there any vulnerabilities in the way you deal with information relevant to your work that may facilitate this threat or make it more damaging?
- **Where**: What aspects of the physical spaces around us (e.g. buildings, vehicles, private property) may make this threat more probable or more damaging? In the case of an office raid and theft, for example, having weak locks on the doors would be a vulnerability.
- **Psychological, emotional and health vulnerabilities:** in the context of this threat, how might stress, tiredness etc. affect you? What gaps or vulnerabilities exist in your well-being practices that may make this threat more likely, or more damaging?

If you wish to record the results of the exercise in writing, you could use a format like the one below:

Threat	[Title of the threat]			
Summary	[Brief description/summary of the threat]			
What	**Target**	**Adversary**	**How**	**Where**
Describe what happens if the threat is carried out (if required, subdivide the threat into its components below).	Specify what/who is the target.	Who is the entity behind this threat?	What information is necessary to carry out the threat?	What are physical spaces in which the threat can manifest?
1)				
2)				
3)				
Psychological, emotional and health impacts				

Identifying the gaps in our security practices can be unnerving but it's an important step in developing the wisdom which will help us to build better security plans. Once we have identified these gaps, we can consider what resources and knowledge we need to build and develop plans and agreements with clear objectives with regard to security.

Identifying new capacities

By now, we should have a good idea of the threats we face, our capacities relative to each of them (including our existing practices) and our vulnerabilities relative to each of them, which should also highlight where there are gaps and room for improvement in our practices. Basing ourselves in this analysis, we can now identify **new capacities to build** in order to improve our well-being in action.

It is useful, therefore, to carry out an initial brainstorm of these new capacities. In the following Chapters, we will explore some of the dynamics around how to develop and implement them.

3.1c Exercise

Brainstorming new capacities

Purpose & Output

In this exercise, you can consider each of the threats you identified and prioritised in **Section II | Explore**, your capacities and your vulnerabilities in order to identify the new capacities you need to build in order to maintain your well-being in action.

Input & Materials

To carry out this exercise, you need to have identified and prioritised threats in **Exercise 2.6b**, and the outputs from **Exercises 3.1a** and **3.1b** above.

Format & Steps

Reflect on the threats you face and your existing capacities and vulnerabilities identified in the previous exercises. You may want to write down your answers in a format such as in **Appendix D.**
Here, you will attempt to 'brainstorm' the new capacities you want to build. Consider the following questions which may help you identify them:

- **Who/what** is under threat? What new capacities should the person or people under threat build in order to reduce the likelihood or impact of the threat identified?
- **Who** is behind the threat? How might you try to influence the cost-benefit analysis of the people or institution who might be behind the threat identified? Is there any way you can improve their tolerance or acceptance of our work, or deter them from acting against you?
- **How:** What information is necessary for them to carry out the attack? How can you further protect the sensitive information about your work and prevent it from falling into the wrong hands?

Format & Steps

- **Where:** How can you increase the security capacities of the physical spaces around us (e.g. buildings, vehicles, private property) in order to make this threat less likely or damaging?
- **Psychological, emotional and health considerations:** In the context of this threat, what practices can you build to reduce stress and tiredness in order to be more aware and react more creatively to the threat?

At this point, it may be a good idea to collate your notes from all the previous exercises to get a clear idea of your current security situation and some of the new capacities you require to deal with the threats you face.

In the next Chapters, we will consider some of the dynamics around building these new capacities and developing them into an overall security strategy and set of security plans.