4. SECURITY INCIDENTS

> **CHAPTER 1.4** OF THE NEW PROTECTION MANUAL
SECURITY INCIDENTS: DEFINITION AND ANALYSIS

LEARNING OBJECTIVES

> Learn to notice, identify and assess security incidents.

> Learn to react to security incidents.

KEY MESSAGES

> All threats are security incidents, but not all security incidents are threats.

> Security incidents represent 'the minimum unit' of security measurement and indicate resistance to, or pressure on, the work of HRDs: they might be considered to constitute a sort of "feedback" which can help improve HRDs' security management.

> Security incidents should be registered, shared, and assessed and, when relevant, proper action needs to be taken.

THE SESSION

CHALLENGES THAT MAY ARISE DURING THE SESSION :

→ Participants may mistake threats for security incidents.

→ Participants may find it hard to react to security incidents when they only have a few elements to assess them.

→ Taking into account the specific protection needs that women HRDs may have (in terms of threats, vulnerabilities and capacities, incidents, etc.).

→ Taking into account the particularities of any other relevant social category when assessing risk (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.).

THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
10´		**Introduction:** • Objectives and structure of the session	Have the points ready on a flipchart or PowerPoint slide.
50'	60'	**Identifying security incidents.** • Explain the distinction between threats and security incidents (NPM, pp. 45-46). • Case analysis. • Identifying security incidents in your own environment (optional activity: adjust the timetable if you do it).	Print-outs of cases to be distributed to participants. Flipchart. Markers.
50´	110'	**Assess and react to security incidents.** • Explain the three steps for dealing with security incidents. • Role-play.	The three steps printed out on paper or written down on flipchart/PowerPoint slide. Sample security incidents for the role-play.
10´	120'	**Conclusion**	
		TIME KEEPING: CALCULATE 140´ (2 HOURS 20 MINUTES), INCLUDING A 20´ BREAK	

LEARNING ACTIVITIES

IDENTIFYING SECURITY INCIDENTS

CASE ANALYSIS

Choose one of the following activities (case analysis 1 or 2) or both (in which case you might not want to go through all five examples of case analysis 1).

→ Participants might confuse threats with security incidents. See Tips for Facilitators – Identifying threats (Chapter 5.3, above).

→ This exercise will be useful only in highly insecure contexts in which HRDs are at clear risk and willing to share some information on the topic (it might even be useful to collect information about real incidents for reporting purposes, if participants agree). Otherwise there may not be enough incidents to be shared, and the timeline will not be useful in illustrating the point. If you are not working in a context similar to this one, you may skip this exercise and proceed to the next.

→ **CASE ANALYSIS 1**

Participants work in groups and each group receives a sheet containing the following situations to analyse. Later, discuss the results in the plenary.

Choose the correct answer for each situation and explain your choice:

A. It is a security incident.

B. It is a threat.

C. It is just a theft (mobile phones are frequently stolen).

1.1 *I am at the bus stop, waiting for the bus and talking on my mobile phone . A man approaches me from behind, takes my mobile phone and runs away through the crowd. I recall he had been looking at me some minutes earlier. I also noticed that there were other people talking on mobile phones but that he targeted me. Now I am worried because I stored people's numbers on the phone.*

1.2 *I am walking to my office. At some point I look across the street and realise that someone is staring at me. Suddenly, the man mimics shooting at me with his hand in the shape of a gun. I carry on walking and reach my office without any problem.*

1.3 *I am about to enter my office when I realise that the door is open and that the office has been broken into during the night. The office is a mess. A few computers have been stolen, but some files related to sensitive cases are still on the desks.*

1.4 *My office has been broken into. In the middle of the mess, I find this note: "Next time, we'll take it to the next stage".*

1.5 *I am walking in the street. I cross the street at the next corner. A motorbike going very fast almost knocks me over. There are two men on the bike. The one sitting on the pillion seat seems very upset and tells me to look out when crossing the street and that next time they won't stop.*

→ To help you ensure discussions remain focused on key elements for understanding the distinction between threat and security incident, consider the following model answers to case 1.1. You can build on these for the other four situations:

- If a group chooses answer a): With the information we have, could we not consider this to be a case of simple theft? In truth, you can't be sure whether it is a simple theft or a security incident. As it could be a targeted action, the theft should be classified as a security incident. You have to take all necessary measures to mitigate the risk caused by the theft of private phone numbers and the possible misuse of the phone (in case the thief sells it on the black market or impersonates you for any illegal purpose). If it is just a theft, it is unlikely that anything serious will happen. But when in doubt, you have to react according to the worst-case scenario as this allows you to take better security measures to face the eventual consequences of the theft. So the answer is correct, but for different reasons.
- If a group chooses answer b): See above: Identifying security incidents and threats.
- If a group chooses answer c): Again, the question is whether it is a simple theft or a security incident. You could consider this event as a simple theft, but how can you be sure that, even if the phone was taken without violence or physical harm being caused, it was not an intentional theft associated with the victim's work as an HRD? As you can't be sure (and note, no other mobile phone user near you was mugged), it could well be intentional targeted action, and this is why the theft has to be considered a security incident. As for answer a) it is important to take all necessary measures to mitigate the risk caused by the theft of private phone numbers and the possible misuse of the phone.

→ **CASE ANALYSIS 2**

Read the case with participants and discuss it in the plenary :

A, B, C and D work at the same HR NGO. They are writing a report about police brutality, which will be launched publicly in two weeks' time. On Monday, A goes home from work and notices someone standing opposite the office smiling at her. She dismisses the incident and assumes the person is just being friendly.

The next day, B has lunch in a café next to the office and a man comes in after him, sitting down at a table which is very close to his, even though the café is empty. B dismisses the incident.

On Wednesday evening, C leaves the office for home. A man stops her outside the office and asks for directions. The man also asks her whether she works there and what kind of work she does. C gives the man evasive answers and goes home. She dismisses the incident and doesn't think about it anymore.

On Friday, D, who likes a drink, goes from the office straight to a nearby bar. After five beers he starts a long chat with a friendly stranger in the bar. At some point D asks the stranger to keep an eye on his bag while he goes to the toilet. When D comes back, the stranger is gone. His bag is still there, with the barman, so D thinks there is no problem. When he gets home a few hours later D realises that his office keys are not in his bag. He wonders if he left them in the office and, being tipsy, decides to bother with that the next day. In the morning he receives a phone call, telling him that someone broke into the office last night.

→ If you want to add a bit of humour, give this answer as a joke: "No, the moral of the story is not that you shouldn't have a drink!" Then listen to their answers. Later, explain that even though it is not up to facilitators to tell people not to drink, it is important when dealing with security to realise that drinking or doing drugs can increase risk as, for example, it lowers levels of alertness and makes people careless. The lesson, of course, is that security incidents need to be shared and analysed. In this case, many security incidents had occurred but they were not discussed, so D did not realise that he was vulnerable and at risk when he went to that bar, even though his behaviour there was careless.

→ Assessing and reacting to security incidents (the role-play)

- The idea is that participants should follow the three basic steps for dealing with security incidents. Only guide the role play necessary. The first formal step consists in registering the incident (which participants might skip). Then the analysis should identify the facts surrounding the security incident, its possible authors and sources (which aspect of the organisation's or HRD's work is related to this incident), and its objectives (to gather information, but for what purpose?). Finally, participants need to decide on how to react to the incident: security measures to be adopted, implications for the security plan, actions to be undertaken, etc.
- If necessary, remind participants that they also need to take care of the victim of the incident.
- Conclude the role-play by asking the participants to identify the key points of the role-play.

IDENTIFYING SECURITY INCIDENTS

After the exercise with cases 1 or 2, ask participants to reflect on incidents that might have occurred in their own working environments and that remained unnoticed or that they did not attach much importance to. Underline that it is important to take into account every single incident, no matter how insignificant it may seem. Minor security incidents are often linked to each other and may pave the way for aggressions or more serious security incidents. Be sure to manage the emotions that may be linked to this exercise and ensure that no one is blamed for not reacting or reporting an incident or threat.

Next, distribute cards (red, yellow and green) and ask participants to write down any security incidents that may have occurred within the past year (one incident per card). Serious incidents (which are not necessarily threats) go on the red cards, medium intensity incidents on the yellow ones, and low intensity incidents on the green. Tell participants they need to be concise. They will have time to explain the incidents in more detail during the plenary session.

Use several flipcharts to draw a timeline on the wall representing the year. Write down each month of the year along the line. Ask participants to place the cards with their security incidents along the same line as they remember them occurring. As the participants explain the details of their security incidents, the facilitator should try to guide them in the identification and classification they have given each incident.

At the end of the exercise, support the group in summarising the insights gained regarding the links between different incidents, the information gathered on the interests and intentions of the potential aggressor, and the importance of recording and analysing security incidents.

ASSESS AND REACT TO SECURITY INCIDENTS

Guide participants through the three steps for assessing and reacting to security incidents, as outlined in **NPM (Chapter 1.4, pp. 47-50)** (you can prepare a presentation or write the steps on a flipchart). Then work on this topic with a role-play.

→ **ROLE-PLAY (30 MINUTES)**

Story:

A member of your organisation is walking in the street when she notices someone following her. She changes pavement and keeps walking. The man following her does the same. She then turns left and starts walking quicker. She does not see the man anymore and decides to go to the office to drop off a few documents. She is unsure about whether she was actually being followed, so she mentions nothing to her colleagues. When she leaves the office to go back home, having hardly reached the next block, she notices the same man, sitting in a white van with no number plates. She decides to go back to the office immediately and inform her colleagues. All staff members present in the office gather to discuss the incident and decide how to react.

Actions:

Tell participants to simulate a meeting and apply the three steps for dealing with security incidents

Roles:

One person is the witness of the security incident. The other participants play the role of staff members.

CONCLUSION

Close the session by asking participants to recall the key learning points of the session.

Insist on the key messages by coming back to examples or problems that arose during the session.

Replace the session in the context of the security management process. Remind participants of the importance of security incidents (see key messages).

Although security incidents are not necessarily integrated in the risk equation, they must be considered as an indicator of the impact of the defenders' work and their security. Thus, security measures need to be adapted to the security incidents suffered by the organisation.

ADDITIONAL RESOURCES

- Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- FLD. Op. Cit. Chapter 6.
- Comité Cerezo Mexico et al. Op. Cit. Chapter 2. (pp. 31-35).