

# 10. INFORMATION MANAGEMENT AND DIGITAL SECURITY



- > **CHAPTER 1.11** OF THE NEW PROTECTION MANUAL  
SECURITY IN COMMUNICATION AND INFORMATION TECHNOLOGY
- > **CHAPTER 3.3** OF THE NEW PROTECTION MANUAL  
SECURE MANAGEMENT OF INFORMATION

This chapter will prove useful for facilitators if risks to the security of digital information kept by defenders have been identified either during the pre-training assessment or during the training itself. In any case, this session is principally intended to raise awareness about a specific aspect of information technology (IT) security (see objectives below). Depending on the digital risk profile of the organisation, their training needs and the setup of the capacity building process, this can either be done as part of one training session dealing jointly with the interlinked dimensions of physical and digital security or as an introduction to a separate, more detailed, digital security training module. **However, facilitators need to ensure that the risk analysis carried out by the HRDs encompasses both dimensions and that plans to build capacity reflect the links between them. Otherwise the sessions will not be relevant or responsive to the risks faced by HRDs.**



## LEARNING OBJECTIVES

- > Raise participants' awareness about the importance of IT security, with a focus on the risks associated with the loss and theft of data.
- > Indicate resources that will help HRDs improve the security of their information.



## KEY MESSAGES

- > Risks to the security of information held by HRDs may come not only from technical failures and targeted attacks intended to obtain access to, or to destroy, the information they hold, but also from careless communication practices.
- > Protecting access to information and regularly backing up information can reduce the risk of data being lost or stolen.

## THE SESSION

### ⚠ CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Facilitators ought to have a minimum understanding of digital security tools (at user level) and in particular those that can assist in minimising the risk of losing data and unauthorised access to it.
- Defenders may be using computers and other devices regularly but still have only a very basic understanding of how they function. Keep all discussions as simple as possible and avoid technical terms that may be confusing or easily misunderstood. If this is not possible, explain the terms in simple, non-technical language and consider using illustrations. Ensure these explanations are visible throughout your sessions for further reference.

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
05'	5'	<b>Introduction:</b> • Objectives and structure of the session	Have the points ready on a flipchart (or PowerPoint slide)
10'	15'	<b>Risks to communicating securely</b>	Flipcharts
45'	60'	<b>Activity:</b> Data backup and protection against unauthorised access	Flipcharts Sticky Post-its
		<b>Guiding participants through the use of digital security tools (optional activity)</b>	Laptop Flash drive (USB key) with latest installation version of "Security in a Box" tools

**TIME KEEPING: CALCULATE 60' (1 HOUR) + \* AND A 20' BREAK**

## LEARNING ACTIVITIES

This session looks principally at the risk of data loss (failure to make back-ups and misappropriation of information by perpetrators) and helps participants to identify current vulnerabilities related to the way they manage information stored on various devices: This information is called "**Data at Rest**". It focuses on simple yet fundamental procedures, as well as possible digital and non-digital tools and measures to increase HRD capacities to manage risk.

Facilitators can find learning materials in the [NPM](#) that they can use to help them prepare this session (see [Chapters 1.11 and 3.3](#)). As threats and digital information protection technologies evolve at a very fast pace, facilitators are encouraged to familiarise themselves with other materials on the topic. At the end of this section, there is a non-exhaustive list of additional resources for further reading.

### RISKS TO SECURE COMMUNICATION

To introduce the topic, the facilitator might wish to begin by asking participants what means they use to communicate with their colleagues and to other people outside their organisation/community. Write down a list of the means of communication mentioned by participants on a flipchart. In case it is not mentioned, remind them that talking face-to-face is perhaps the most common way to communicate (sometimes inadvertently) sensitive information about their work. Thus, information security and protection is not just a question of sophisticated communication technologies.

Next, brainstorm with participants on the various ways in which information or communications can be legally accessed but also manipulated: e.g. when talking face to face or via mobile phone or as a consequence of aspects of the physical security of the office. Use the information in [NPM \(Chapter 1.11\)](#) for inspiration.

If participants consider they are at risk of being listened to during face to face conversations or when using mobile phones, recommend that they develop protocols for handling sensitive information during communications of this kind as part of their security plan. You can point to the above chapter for guidance.

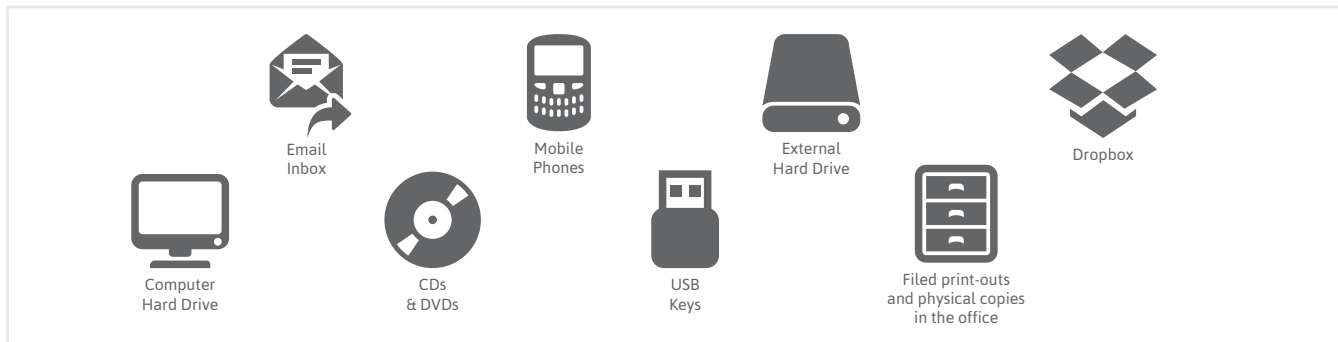
Move towards a different aspect of information security by asking participants how important the information is that they keep in digital formats: emails, reports, partner and beneficiary contact details, etc. If participants assign significant importance to this information, ask them to identify (or indicate for them, if they are struggling) ways in which they risk losing this information (e.g. through a technical fault, loss or theft of equipment, or unauthorised access like hacking).

 **ACTIVITY: DATA BACKUP AND PROTECTION AGAINST UNAUTHORISED ACCESS<sup>1</sup>**

Depending on previous sessions with participants and the discussions on risks relating to information security, make a link to the risk of data loss and what it could mean for HRDs and the persons they work with and for. Ask them what ad hoc strategic measures they currently have in place to avoid the loss of their data.

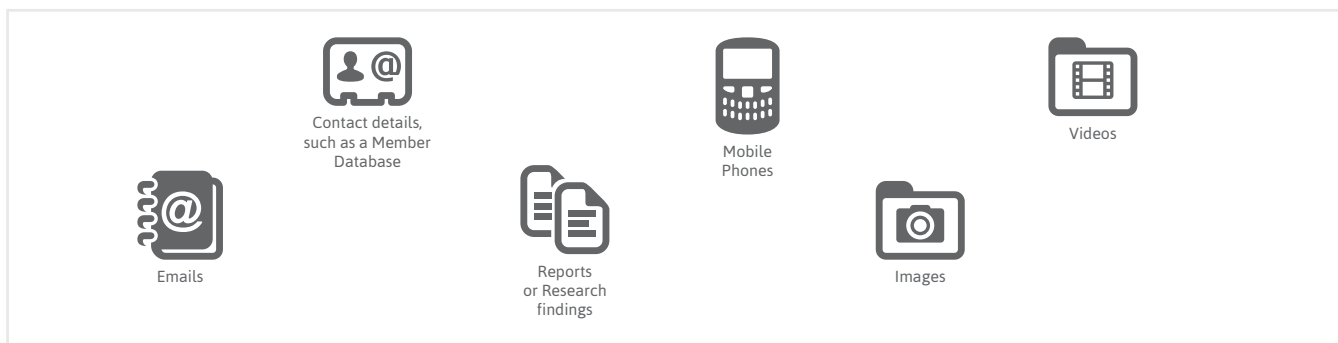
Prepare two flipcharts taped together and draw a matrix (see below) and stick this up in a clearly visible place on the wall. Explain to participants that this is an information mapping exercise that seeks to visualise **what** kind of information they have and **where** it is stored. This will form the basis for developing a strategy to reduce the risk of data loss.

Start by asking participants to list the different places where their information is stored. If no suggestions are forthcoming, you can prompt with the following:



Add the locations mentioned by participants to the top row of the matrix. Then ask participants what type of information or data they store in each of these places.

For example:



Write one example on a card/post-it and place it in the relevant part of the matrix: e.g. reports on the hard drive of the computer.

Ask whether there is another copy of this data somewhere else. If there is, you can use a different-coloured post-it and place it wherever they keep the duplicate. You can use this moment to differentiate between **master copies** and **duplicates** or **back-ups**. (In the example below orange indicates master copy and light grey indicates duplicate).

<sup>1</sup> This activity has been adapted from Samir Nassar, Daniel Ó Clunaigh, and Ali Ravi from Tactical Technology Collective for the LevelUp project. Facilitators are also encouraged to read **NPM Chapter 3.3** for background information.

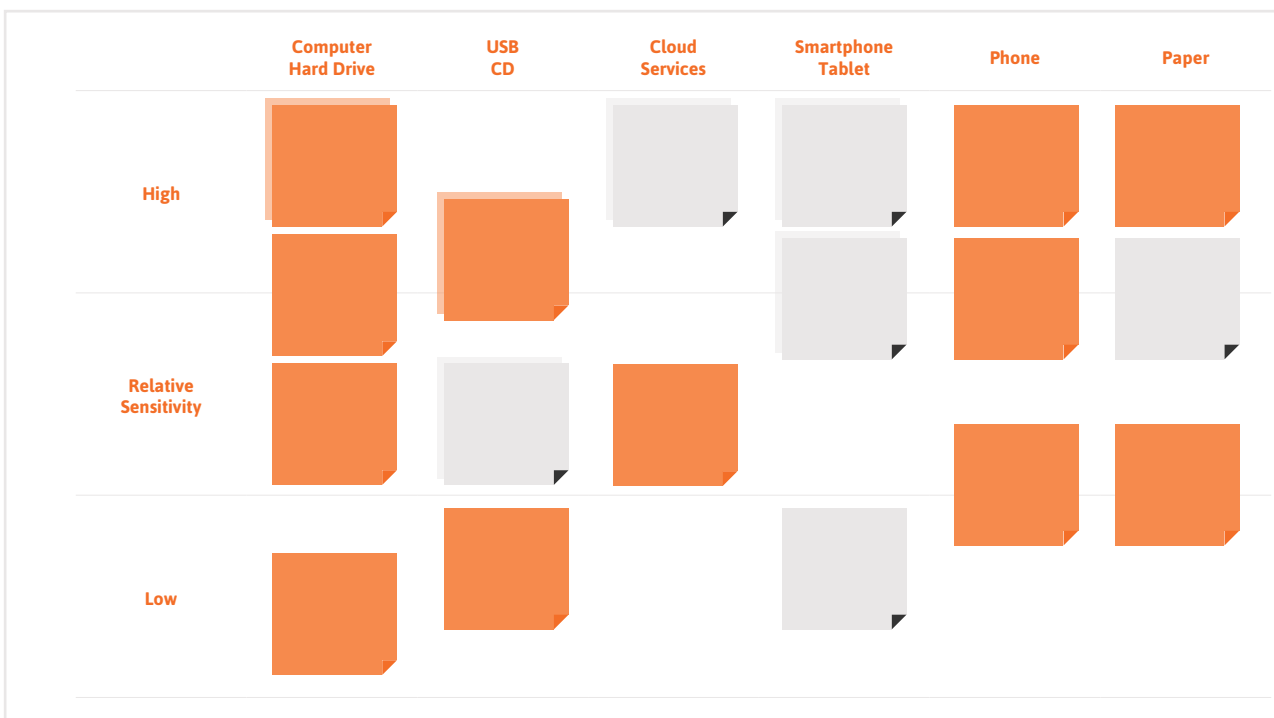
Repeat this process with one more dimension: data sensitivity (meaning data that, if lost or misused, might cause considerable harm either to the HRDs or to the people they are working with, such as victims of gender-based violence). Introduce a second (vertical) axis representing sensitivity. The higher on the chart a card/post-it is placed, the more sensitive the data it represents. Place the two cards/post-its on this axis representing their relative sensitivity. If you have limited time available, you are free to reduce this part of the exercise to one or two examples.



Next, form small groups: one group per organisation when participants come from different organisation or by thematic areas when all come from the same one. This activity can also be conducted as a brainstorming exercise in plenary if all participants are from the same organisation.

Allow 5-10 minutes for this exercise. It is advisable for the facilitator to observe each group and identify interesting characteristics (e.g. where there is a particularly large dependence on one device or copies/back-ups are few, etc.). By the end of the exercise each team should have completed a matrix.

An example might look something like this :



Explain that this matrix gives an idea of where the data is located. Ask whether this is all the data their organisation/community generates. The answer is, of course, that it is not – it is only a small percentage.

Then, take the matrix of one of the teams as an example. If trust levels among all participants allow, read out the information the group keeps on their computer's hard drive, which is usually the fullest.

To illustrate the vulnerability this entails, ask participants what might cause a computer to stop working.

- Virus or malware attack destroys data stored in a computer
- Stolen or confiscated computer
- Infrastructural problems like power failure damages a computer


You can ask participants to raise their hands to indicate which of the above has affected them in the past.

Now ask what would happen to the data if one of the above events were to occur. To emphasise the impact, you can dramatically remove each of the cards/post-its from the column and throw them on the floor. The remaining cards on the matrix represent all the information they would be left with.

Ask participants to think about what could be done to avoid this? The answer is likely to be that they should keep more copies in different locations. Point out that this is what we call backing up!

Now, if time allows, turn to the matter of the sensitivity of data. If possible, take the example of another team's matrix. If the exercise has been carried out in plenary, pick another column on the matrix. Ask participants what the impact would be if their phone/hard drive/USB key were stolen. Take the cards/post-its from the respective column, but keep them in your hand and read them. This illustrates that now someone else is in possession of the information held on the device. Ask what they could do with it and what situation the HRDs would be left in.

Drawing on the previous activity on data backup, ask participants to identify a minimum of three to five things that need to be done to reduce the vulnerabilities they have identified. These steps might be digital: e.g. mention Cobian Backup as well as non-digital solutions such as fundraising to buy back-up devices, develop backup protocols, etc. Depending on the composition of the training group, ask them to do this on organisational (for homogeneous groups) or individual level (heterogeneous groups).

-  → This activity is in essence a risk analysis concerning the data HRDs possess – and might lose – and helps to identify existing vulnerabilities.
- The ideal circumstances for this exercise are a training group with high levels of trust or that can easily be divided into relatively homogenous groups. For groups where trust levels are low or for heterogeneous groups who do not know each other well and may not be comfortable letting others know what information they hold and how it is kept, the exercise needs to be modified to make it more generic while maintaining the learning points.

#### **GUIDING PARTICIPANTS THROUGH THE USE OF DIGITAL SECURITY TOOLS (OPTIONAL ACTIVITY)**

If carried out, this part of the session is intended to address the vulnerabilities that have been identified and to strengthen participants' capacities to face the risk of data loss and unauthorised access both to **"Data at Rest"** (data stored on a device: see above) and **"Data in Motion"**.

**"Data in Motion"** refers to the exchange of information, e.g. via internet, email, mobile phone or social media, which HRDs frequently use for their work and to exchange information with stakeholders. One of the principal risks involves the possibility that opponents might gain unauthorised access to sensitive information, either by hacking into user accounts or by eavesdropping or intercepting information by other technical means. By helping HRDs identify existing vulnerabilities in this area you support them in establishing

procedures to create and maintain strong passwords, use safer (i.e. encrypted) channels of communication and/or ensure information itself is exchanged securely, e.g. by encrypting it.

To address vulnerabilities identified during these exercises, facilitators will want to be familiar with the following:

- Creating strong passwords (for email accounts, computers, files etc.)
- Encrypting information stored on devices and in motion
- Maintaining privacy for internet communication
- -Backing up information

Facilitators are encouraged to introduce participants to these digital security tools using the resources found at <https://securityinbox.org>



To work with the resources in <https://securityinbox.org>, facilitators are advised to:

- Be conversant with the use of the tools yourself by making it a part of your own security strategy: strong password practices, encrypting information stored on devices or sent via the internet or mobile networks, and regular data back up.<sup>2</sup>
- Carefully read through the corresponding section of the “How to” Booklet on the website <https://securityinbox.org/en/howtobooklet>. This will give you relevant information on which vulnerabilities a specific tool can address, which it illustrates using case studies that can be usefully adapted to the context of your participants.
- Be aware of the different features that the tools provide, and introduce only those that respond to the risks identified by your participants. This is to avoid overloading participants with information they might never apply.
- Make sure to download the latest version of the tools you want to introduce from the “Security in a Box” website ahead of the training session and to store them on your computer or on a portable device for your demonstrations so that participants can copy them. This will guard against possible delays should the internet connection during the training session not allow participants to download the software quickly.
- When selecting the venue for the training session, consider whether there is a regular power supply and back-up options, such as generators, to ensure the training is not interrupted by power cuts.
- Before the session, make a test run of the installation and all components you hope to introduce to be sure they function on your computer. This is essential for you to be able to guide participants through the installation and features via a projector.
- To avoid spreading computer viruses, ask participants whether they have an antivirus programme and to make sure it is up to date. You could also make a version of the free Avast antivirus software available for participants who have no antivirus or whose programme is not up to date.
- If participants use their personal or work computers for the training session (rather than hiring computers that have been serviced and cleaned of malware and possible non-essential applications) it is likely that it will be difficult to install the tools or to complete certain tasks, because of the different settings. As you are not a technician and time available for the session is limited, refrain from trying to fix these problems during the session. Instead, ask participants affected to work together with one of their colleagues to ensure that the session objectives can be met for the entire group.

<sup>2</sup> Considering the fast developments in this field, maintain an understanding of what is happening in terms of digital security and privacy issues by keeping updated via the Security in a Box website, AccessNow ([www.accessnow.org](http://www.accessnow.org)), Ono (<https://onorobot.org>) and others. Where possible, attend digital security training not only to improve your use of tools or learn about others, but also to improve your facilitator skills in this area.

- It is desirable to have at least one computer per two participants to allow them to follow your instructions as well as practice the tools by themselves.
- Use the respective section from the “Hands on Guides” to prepare for the demonstration of the tools (<https://securityinabox.org/en/handsonguides>). Practice this in advance and anticipate questions. Keep your language simple and illustrate the relevance of the tools to the risks identified by defenders.<sup>3</sup>
- When introducing the tools, ask participants to close all other applications and follow you for the first demonstration via the projector screen. Then ask them to do the same themselves on their computer following your guidance on screen. Finally, ask them to repeat the same procedure without guidance. The more opportunity they have to practice the tools themselves, the deeper the learning experience.
- The use of digital security tools may be a challenge to quite a number of HRDs. Point out the benefits of using the tools in response to their identified risks. Underline that the more they use the applications the more comfortable they will feel with them.
- Point participants to the resources in <https://securityinabox.org> for further tools and guidance. All these tools are free and the toolkit is regularly updated.
- The Digital Security First-Aid-Kit for Human Rights Defenders outlines specific risk scenarios and provides guidance on immediate measures to remedy the situation. It also provides links to additional resources such as Security in a Box and others (<https://www.apc.org/en/irhr/digital-security-first-aid-kit>).

<sup>3</sup> Level Up! is an upcoming resource for trainers in digital security that will provide information in how to prepare and deliver digital security training sessions. Refer to <http://level-up.cc> for inspiration and guidance.

## CONCLUSION

- > Remind participants that the activity on data backup and theft/loss is aimed at providing them with insights into where their data is stored, which of it is sensitive, and which needs to be protected from unauthorised access, or backed up because it is currently only stored in one place. Encourage participants to recall key learning points and further training needs, which they should include in their action plans.
- > Should you introduce the use of specific digital security tools, let participants recall which identified risks they address and why they consider them worth using. To ensure application of the tools, consider developing assignments or “homework” so participants can practice and become comfortable with their use.



## ADDITIONAL RESOURCES

- > Association for Progressive Communication (2013). Digital Security First-Aid Kit for Human Rights Defenders. <https://www.apc.org/en/irhr/digital-security-first-aid-kit>
- > Front Line Defenders (2009). Digital Security and Privacy for Human Rights Defenders. [http://www.frontlinedefenders.org/files/en/eseaman.en\\_.pdf](http://www.frontlinedefenders.org/files/en/eseaman.en_.pdf)
- > Tactical Tech Collective. Me and My Shadow. <https://myshadow.org/>. Resources and tools limiting which information one leaves behind when using the internet.
- > Level Up! Facilitator's toolkit for digital security trainers. <http://www.level-up.cc>.
- > Tactical Tech Collective and Front Line have developed the reference toolkit <http://securityinabox.org> available in book form, on DVD and online. You are recommended to use of the online version as it has the most up-to-date versions of the software. Securityinabox.org addresses the following areas:
  - [How to protect your computer from malware and hackers](#)
  - [How to protect your information from physical threats](#)
  - [How to create and maintain secure passwords](#)
  - [How to protect the sensitive files on your computer](#)
  - [How to recover from information loss](#)
  - [How to destroy sensitive information](#)
  - [How to keep your Internet communication private](#)
  - [How to remain anonymous and bypass censorship on the Internet](#)
  - [How to protect yourself and your data when using social networking sites](#)
  - [How to use mobile phones as securely as possible](#)
  - [How to use smartphones as securely as possible](#)







**Protection International AISBL**

11 Rue de la Linière  
1060 Brussels – Belgium

**+32 2 609 44 05**

**<http://protectioninternational.org>**