Image not found or type unknown

The data life cycle as a way to understand risk [deepening activity]

Look at risk assessment from the perspective of the data life cycle. Activists, organisations and movements all deal with data – from gathering/creating/collecting data to publishing information based on data.

Introduction and mechanics for a general workshop

image-1605640472202.png
Image not found or type unknown

This learning activity is about looking at risk assessment from the perspective of the data life cycle.

Activists, organisations and movements all deal with data – from gathering/creating/collecting data to publishing information based on data.

There are two main approaches to the mechanics of this activity:

- The **general workshop** is for a general digital security workshop, where the participants come from different organisations and/or don't belong to any organisations.
- The **organisational workshop** is meant for a specific group and its staff. The general context for this type of workshop is that different teams within an organisation come together to to do a risk assessment of their organisational data practice and processes.

The learning objectives and the general topics/themes covered in both approaches are the same, but the facilitation methodologies and techniques will need to be adjusted for two different kinds of workshop scenarios.

Learning objectives

Through this activity, the participants will be able to:

- Understand risk and security considerations in each phase of the data life cycle.
- Apply risk assessment frameworks to their personal and/or organisational security.

Who is this activity for?

This activity is meant to be for individual activists (in a general risk assessment or digital security workshop), or for a group (an organisation, network, collective) undergoing a risk assessment process. There are two mechanics and approaches for this activity, depending on whether it is a general workshop or a workshop for a specific group.

It can also be used as a diagnostic activity in order to prioritise which practices or tools to focus on for the rest of a digital security workshop.

Time required

This depends on the number of participants and the size of the group. In general, this activity takes a minimum of four hours.

Resources

- Flip chart paper
- Markers
- Projector to present the data life cycle and the guide questions and for participant share-backs, if needed.

Mechanics

(This is for a general risk assessment or digital security workshop, where activists from different contexts come together in a training. The learning objectives remain the same but some of the training and facilitation tactics would differ from a workshop for a more established group of people.)

Phase 1: What do you publish?

In this part of the activity, the participants are asked: **What do you publish as part of your work as an activist?**

The point here is to start with the most obvious part of the data life cycle – processed data that is shared as information. This could be research reports, articles, blog posts, guides, books, websites, social media posts, etc.

This could be done in plenary, popcorn style. This is when the facilitator posts a question and asks for short and brief answers from the participants – like corn popping in a pan!

Phase 2: Presentation of the data life cycle and security considerations

The presentation is aimed at reminding the participants about the data management cycle. The key points for the presentation can be found here *(see cycle-basics-presentation.odp)*.

Phase 3: Reflection time about personal data life cycles

Group the participants according to what they publish. Ask them to choose a specific example of something that they have published (an article, a research report, a book, etc.), and ask them to form groups based on similar work.

Here, there will be time for each of them to track the data life cycle of that published output, and then time as a group to share their reflections.

Reflection time should be about 15 minutes. Then group discussion would take about 45 minutes.

The guide questions for individual reflection time will be the considerations in the presentation.

For the group work, each group member will share the data life cycle of their published work.

Phase 4: Share-back and security considerations

Instead of having each group report back, the trainer-facilitator asks each group questions that will surface what was discussed in the groups.

Here are some questions you may use to debrief on the reflection time and the group discussion:

- What are the data storage devices that were most common in the group? What were the ones that were the only one used?
- What were the differences and commonalities in access to the data storage in your group?
- What about data processing? What tools were used in your group?
- Did anyone in the group publish something that put them or someone they know at risk? What was it?

- Has anyone in the group thought about archiving and deletion practice before today? If so, what were the practices around this?
- Were there safety and security concerns at any part of your data life cycle? What are they?

Synthesise the activity

At the end of the group presentations and sharing, the trainer-facilitator can synthesise the activity by:

- Pointing to key points made.
- Asking participants for key insights from the activity.
- Asking participants about changes in their data management practice that they learned about during the activity.

image-1605452256072.png
Image not found or type unknown

Mechanics for an organisational workshop

> This is for a workshop for an organisation and its staff.

Phase 1: What information does each unit/programme/team of the organisation share?

Based on the configuration and structure of the organisation, ask each unit or team for an example of one thing that they share – within the organisation or outside the organisation.

Some examples to encourage response:

- For communications units – what are the reports that you publish?
- For research teams – what is the research that you report on?
- For administration and/or finance teams – who gets to see your organisation's payroll? How about financial reports?
- For human resources departments – what about staff evaluations?

> **Facilitation note:** This question is much easier to answer for teams that have outward-looking objectives, for example, the communications unit, or a programme that publishes reports and research. For more inward-looking units, like finance and administration or human resources, the trainer-facilitator may need to spend time on examples of what information they share.

The goal in this phase is to get the different teams to acknowledge that they all share information – within the organisation or outside of it. This is important because each team should be able to identify one or two types of information that they share when they assess risk in their data management practice.

Phase 2: Presentation of the data life cycle and security considerations

The presentation is about reminding the participants about the data management cycle. The key points for the presentation can be found here (see file cycle-basics-presentation.odp).

Phase 3: Group work

Within teams, ask each group to identify one to two types of information that they share/publish.

In order to prioritise, encourage the teams to think about the information that they want to secure the most, or information that they share that is sensitive.

Then, for each type of shared or published information, ask the teams to backtrack and look at its data life cycle. Use the presentation below to ask key questions about the data management practice for each piece of published or shared data.

At the end of this process, each team should be able to share with the rest the results of their discussions.

In general, the group work will take about an hour.

Phase 4: Group presentations and reflecting about safety

Depending on the size of the organisation and the work that each unit has done, give them time to present the results of their discussion to their co-workers. Encourage each team to think about creative presentations and highlights of their discussions. They do not need to share everything.

Encourage the listeners to take notes about what is being shared with them, as there will be time to share comments and give feedback after each presentation.

Realistically, this will take about 10 minutes/group.

The role of the trainer-facilitator here, aside from timekeeping and managing feedback, is to also provide feedback to each presentation. This is the time to put on your security practitioner hat.

Some areas to consider asking about:

- If the data gathering process is supposed to be private, wouldn’t it be better to use more secure communications tools?
- Who has access to the storage device in theory and in reality? In the case of physical storage devices, where are they located in the office?
- Who gets to see the raw data?

As a trainer-facilitator, you can also use this opportunity to share some recommendations and suggestions to make the organisation’s data management practices safer.

Facilitator's note: There is a resource called Alternative Tools in Networking and Communications in the FTX: Safety Reboot that you might want to have a look at to guide this activity.

Phase 5: Back to the groups: security improvements

After all of the teams have presented, they return to their teams for further discussion and reflection on how they can better secure their data management processes and data.

The goal here for each group is to plan ways to be safer in all of the phases of their data life cycle.

By the end of this discussion, each team should have some plans as to how to be more secure in their data practice.

Note: The assumption here is that the group has undergone some basic security training in order to do this. Alternatively, the trainer-facilitator can use Phase 4 as an opportunity to provide some suggestions for more secure alternative tools, options and processes for the group's data management practice.

Guide questions for group discussion

- Of the types of data that you manage, which ones are public (everyone can know about them), private (only the organisation can know about them), confidential (only the team and specific groups within the organisation can know about them) – and how can your team ensure that these different types of data can be private and confidential?
- How can your team ensure that you are able to manage who has access to your data?
- What are the retention and deletion policies of the platforms that you use to store and process your data online?
- How can the team practise more secure communications, especially about the private and confidential data and information?
- What practices and processes should the team have in place in order to preserve the privacy and confidentiality of their data?

- What should change in your data management practice in order to make it more secure? Look at the results of the previous group work and see what can be improved.
- What roles should each team member have in order to manage these changes?

Phase 6: Final presentation of plans

Here, each team will be given time to present the ways that they will secure their data management practice.

This is an opportunity for the entire organisation to share strategies and tactics, and learn from each other.

Synthesising the activity

At the end of the group presentations and sharing, the trainer-facilitator can synthesise the activity by:

• Pointing to key points made.

• Asking participants for key insights from the activity.

• Agreeing on next steps to operationalise the plans.

Presentation

Another way to understand risks in increments is to look at an organisation’s data practice. Every organisation deals with data, and each unit within an organisation does as well.

Here, there are some security and safety considerations for each phase of the data life cycle.

Creating/gathering/collecting data

- What kind of data is being gathered?
- Who creates/gathers/collects data?
- Will it put people at risk? Who will be put at risk for this data being released?
- How public/private/confidential is the data gathering process?

- What tools are you using to ensure the safety of the data gathering process?

Data storage

- Where is the data stored?
- Who has access to the data storage?
- What are the practices/processes/tools you are using to ensure the security of the storage device?
- Cloud storage vs physical storage vs device storage.

Data processing

- Who processes the data?
- Will the analysis of the data put individuals or groups at risk?
- What tools are being used to analyse the data?
- Who has access to the data analysis process/system?
- In the processing of data, are secondary copies of the data being stored elsewhere?

Publishing/sharing information from the processed data

- Where is the information/knowledge being published?
- Will the publication of the information put people at risk?
- Who are the target audiences of the published information?
- Do you have control over how the information is being published?

Archiving

- Where are the data and processed information being archived?
- Is the raw data being archived or just the processed information?
- Who has access to the archive?
- What are the conditions of accessing the archive?

Deletion

- When is the data being purged?
- What are the conditions of deletion?
- How can we be sure that all copies are deleted?

Facilitator’s notes

- This activity is a good way to be able to know and assess the digital security contexts, practice and processes of participants. It is a good idea to focus on that aspect rather than expect this activity to yield strategies and tactics for their improved digital security.
- For an organisational workshop, you may want to pay attention to the human resources and administration teams/units. First, in many organisations, these are usually the staff members who have not had prior digital security workshop experience, so many of the themes and topics may be new to them. Second, because a lot of their work is internal, they may not see their units as “publishing” anything. However, in many organisations, these units hold and process a lot of sensitive data (staff information, staff salaries, board meeting notes, organisational banking details, etc.) – so it is important to point that out in the workshop.
- Pay attention to the physical storage devices as well. If there are file cabinets where printed copies of documents are stored, ask where those cabinets are located and who has physical access to them. Sometimes, there’s a tendency to focus too much on online storage practice, and they can miss out on making their physical storage tactics more secure.

Further reading (optional)

- FTX Safety Reboot: Alternative Tools in Networking and Communications
- FTX: Safety Reboot :Mobile Safety Module
- Electronic Frontier Foundation's Surveillance Self-Defense – while this is largely for a US-based audience, this guide has useful sections that explain surveillance concepts and the tools used to circumvent them.

- Front Line Defenders' Guide to Secure Group Chat and Conferencing Tools – a useful guide to various secure chat and conferencing services and tools that meet Front Line Defenders’ criteria for what makes an app or service secure.
- Mozilla Foundation's Privacy Not Included website – which looks at the different privacy and security policies and practices of different services, platforms and devices to see they if match Mozilla's Minimum Security Standards, which include encryption, security updates, and privacy policies.

image-1605451259399.png

Revision #8
Created 18 April 2023 04:05:18 by Kira
Updated 28 July 2023 14:51:35 by Kira