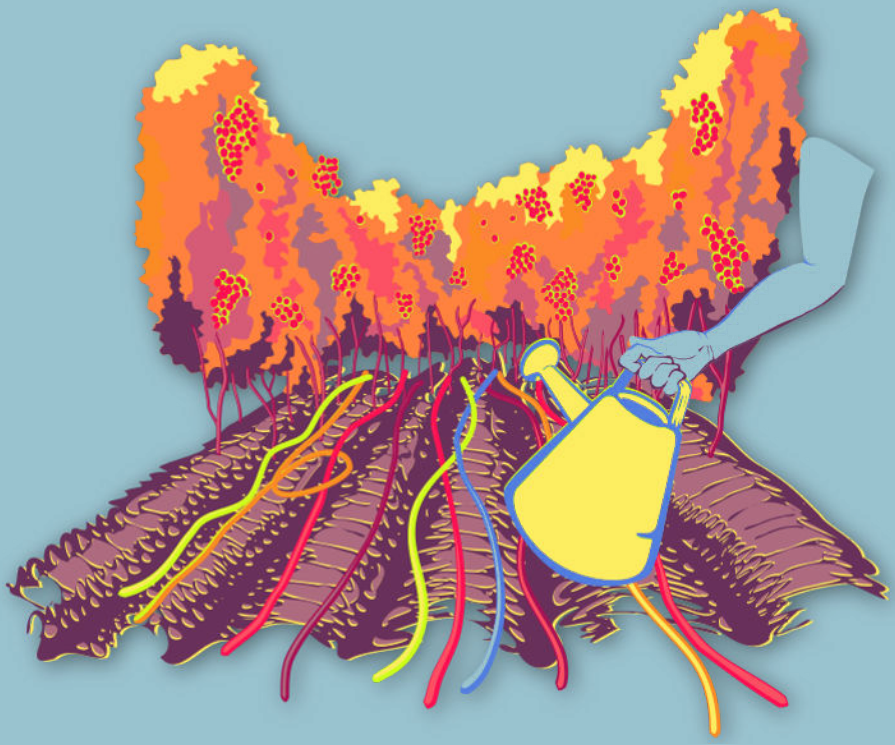

Planning ahead

Planning ahead

https://iwpr.net/

Contents

Organizational security plans and protocols

- **Objective(s):** To facilitate a process for women to develop a security plan and corresponding protocols that they can use to implement digital security measures in their own organization.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Hands-on practice with digital security tools and practices from previous training
  - Who do you trust?[1]
  - Gender-based risk model[2]
- **Related sessions/exercises:**
  - Personal perceptions of security[3]

[1] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/

[2] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/

[3] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/

  - Who do you trust?[4]
  - How does the internet work?[5]
  - Gender-based risk model[6]
  - Digital security plans and protocols: post-training replication[7]
- **Needed materials:**
  - Risk model from Gender-Based Risk Model exercise
  - Printed security protocol templates (see example template below)
- **Recommendations:** This session is best suited for participant groups who come from the same organization or collective, as the activities below are focused on developing an organizational level security plan – the process of designing this together will help support women's ongoing practice and implementation of it. it is crucial to follow-up with participants on the implementation of the plan they create – if possible, connect with them every two or three weeks to check on progress (apart from answering any questions they might send in the interim). be careful not to pressure participants about using specific tools or implementations of them when follow up with them – simply support them and be present with them, responding to any questions or concerns they have and providing recommendations when requested. if participants feel pressured, they may not be forthcoming about whether they've addressed a specific issue and won't feel comfortable sharing actual difficulties when they arise.

[4] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/

[5] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/

[6] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/

[7] https://cyber-women.com/en/planning-ahead/digital-security-plans-and-protocols-post-training-replication/

Leading the session

Part 1 – Return of the Risk Model

1. Begin the session by highlighting the importance of building a risk model before drafting a plan and any protocols. Remind participants that digital security is first and foremost a personal process - if their goal is to draft and implement a digital security plan at an organizational level, explain that it will be a process of:
    - Mapping threats collectively - this can be done over the course of a couple training sessions with the entire team present, however remind the group that remaining aware of and updated on the threats they face will be an ongoing process.
    - Learning the difference between strong habits and unsafe habits of digital security, and remaining up to date on new tools or updates to existing ones.
    - Making implementation decisions together as a team, but also identifying areas where individuals can create and practice their own processes as they see fit.
    - Consistently monitoring the implementation of their organizational digital security plan, ensuring that corresponding protocols are well understood before they are practiced, and troubleshooting any emerging difficulties throughout.

Part 2 – Plans vs. Protocols

2. Explain to participants the difference between a digital security plan and a digital security protocol. The main idea to communicate is that:
    - A plan is an outline of key changes that an organization or collective has identified as requirements for increasing their digital

security. Plans are a defined process, with a beginning and an end.

- A protocol is a set of measures or actions related to digital security that are each connected to a specific activity or process within an organization or collective. Protocols are ongoing practices that remain in effect even when a digital security plan has been fully implemented, and will evolve over time in response to changes in risk and threat environments.

Provide examples of plans and protocols to participants – for instance, activities such as travel or participation in public protests would each have their own digital security protocol; items found in a digital security plan might include an organization having their website audited, verifying that every computer has antivirus installed, and introducing the use of GPG to encrypt emails.

Part 3 – Creating an Organizational Plan and Protocol

3. This session is best suited for participant groups who come from the same organization or collective, as they can take advantage of this opportunity to collaborative develop their plan and protocols as a team. However, if this is the case for only some participants, those who are not part of any organization or group can still participate in the session by working on their own personal plans and protocols.
4. Ask participants to refer to their risk model from the Gender-Based Risk Model exercise, as well as their notes from the Who Do You Trust? exercise. Have them begin making a draft of their security plan - the following format may be useful. Explain to participants each of the sections (a new row should be started for each risk or threat identified):

Threats and Risks	Which threats and risks do we currently face? Which could we potentially face in the future?

Identified Vulnerabilities	Which of our practices as individuals, or circumstances as an organization, could expose us to harm?
Strengths and Capacities	What strengths do we have as organization that give us an advantage in responding to identified threats and risks?
Mitigating Actions	What kind of measures do we need to take in order to mitigate the risks? To be better prepared for identified threats?
Resources Needed	What resources (economic, human, etc.) would we need to implement these actions?
Who Needs to be Involved?	Which areas or people within our organization need to be involved in implementation? Will any sign-off or other permissions be required?

5. Remind participants that although the focus of this training is on digital security, we must always remember to take holistic measures into account. Ask participants to consider which actions need to be taken in terms of physical security and self-care as they draft their security plans and protocols.
6. Then, after participants have finished their first draft of the plan template, ask them to then build a list of their organization's activities or processes that they feel will require individual protocols.
7. Once participants have finished both their draft plan template and their list of activities requiring security protocols, it will be useful to pause so that everyone can share their plans. This presents a valuable opportunity for participants to learn from the approaches of others; however, remember that some may not feel comfortable sharing their organizational or personal vulnerabilities as a matter of trust. To address this proactively, you may want to ask the group to share only the key items for their plan (the 4th column of the template table, "Mitigating Actions") while keeping other information like "Threats and Risks" and "Identified Vulnerabilities" private.

Part 4 – What's Next?

8. Discuss follow-up steps with participants - they will need to have a focused gathering within their organizations to share insights and key takeaways from this session, as well as the Gender-Based Risk Model exercise and the Who Do You Trust? exercise – of special importance from this session will be the list of activities and processes requiring security protocols. This plan will need to be discussed and agreed upon as a team, with realistic dates set for its implementation – while considering these, participants also need to remember that there may be others in their organizations who will require training on digital security practices and/or specific tools for full implementation to be possible.

Digital security plans and protocols

- **Objective(s):** To build on the organizational security plans and protocols session. here, you will present a set of recommendations that can help participants facilitate post-training implementation of their security plans and protocols within their organizations.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Hands-on practice with digital security tools and practices from previous training
  - Organizational security plans and protocols[1]
  - Who do you trust?[2]
  - Gender-based risk model[3]
- **Related sessions/exercises:**

[1] https://cyber-women.com/en/planning-ahead/organizational-security-plans-and-protocols/

[2] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/

[3] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/

  - Organizational security plans and protocols[4]
  - Who do you trust?[5]
  - Gender-based risk model[6]
- **Needed materials:**
  - Slides with key points included below
  - Laptop/computer and projector setup

Leading the session

Part 1 – Mapping Organizational Structures and Barriers

1. Working in pairs, ask participants to describe their organizations:
   - How many people participate in them?
   - How often do they meet?
   - Are there areas or committees that bring different parts of the organization together?
2. Remaining in pairs, now ask participants to share with one another some of the barriers or challenges they anticipate facing within their organizations when presenting their security plans and articulating the need to begin an implementation process.

Part 2 – Facilitating Organizational Implementation

3. Once the groups have finished discussing the points above, share some ideas that can help participants facilitate post-training implementation of their security plans and protocols within their organizations:

[4] https://cyber-women.com/en/planning-ahead/organizational-security-plans-and-protocols/

[5] https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/

[6] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/

- Recommend that they frame this as the beginning of a reflection process - it will take time to get the plan implemented and the protocols developed and tested, and there will be an adjustment period as people get used to these changes. Regardless, they should make sure to emphasize that thinking in a more critical way about organizational security is a positive step.
- Warn participants that they might receive some push-back on the term "protocols" as it may come across as overly technical and intensive; they should remind others in their organizations that protocols are nothing more than an agreement about the specific risks and threats they face, and a commitment to solve them together by putting strategic actions into place for the good of the organization and its mission.
- Underscore the importance of collaboration and inclusion in the implementation process – participants should work with different teams within their organizations on their team-level risk assessments, and have them share the outcomes and next steps with the rest of their colleagues. Emphasize also that it will be critical for participants to hold space for others in their organization to provide feedback on the security plan and protocols – as different people's tasks will be affected in different ways by these new measures, they will want to avoid creating additional difficulty for anybody's work.
- Have participants consider other ways to collectively engage different teams across their organization – one such approach is for them to propose a "digital security commission" that includes representatives (who are empowered to make decisions) from each team or area who are together tasked with overseeing the implementation of the security plan. They can go about this process gradually, focusing first on high-level staff or starting out only with specific teams and then expanding outward. The approach that works best will vary widely by organization.
- Finally - ask the participants to share some of the ideas they have

that could help facilitate the implementation process for their organizations.

Part 3 – Starting the Conversation

4. Share with participants a basic structure for starting this important conversation within their organizations - it could be a set of questions, or a possible training plan of their own with specific sessions and exercises relevant to the organizational risk context.

5. Remind the group to be aware of the logistics involved, time in particular – people within their organization may not have the time to set aside an entire afternoon, day or even longer for training. Changing long-standing habits takes a lot of time and patience, so it's will be more ideal for participants to find ways of building these conversations (or trainings) into existing regular meetings or other gatherings.

   Here is a basic structure that participants could follow to raise awareness of certain topics – this begins with a conversation about why digital security is important for the organization, and then includes sessions (from this curriculum) which go into further detail on basic digital security topics - how participants ultimately choose to have these conversations is up to them:

   - Conversation: Why Digital Security is Important for Our Organization
   - Session: How does the internet work?[7]
   - Session: [Let's start a documentation journal!][]
   - Session: Mobile phones 1[8]
   - Session: Encrypted communication[9]
   - Session: Safe browsing[10]

[7] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/
[8] https://cyber-women.com/en/safer-mobiles/mobile-phones-1/
[9] https://cyber-women.com/en/encryption/encrypted-communication/
[10] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

- Exercise: Gender-based risk model[11]

6. Remind participants that this is just a suggested approach – they should feel free to adjust the sessions and the topics as they see fit. It is important that, as participants work through the implementation process with their organizations, that you make yourself available (to the extent possible) to provide support and answer any question they might have.

[11] https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/