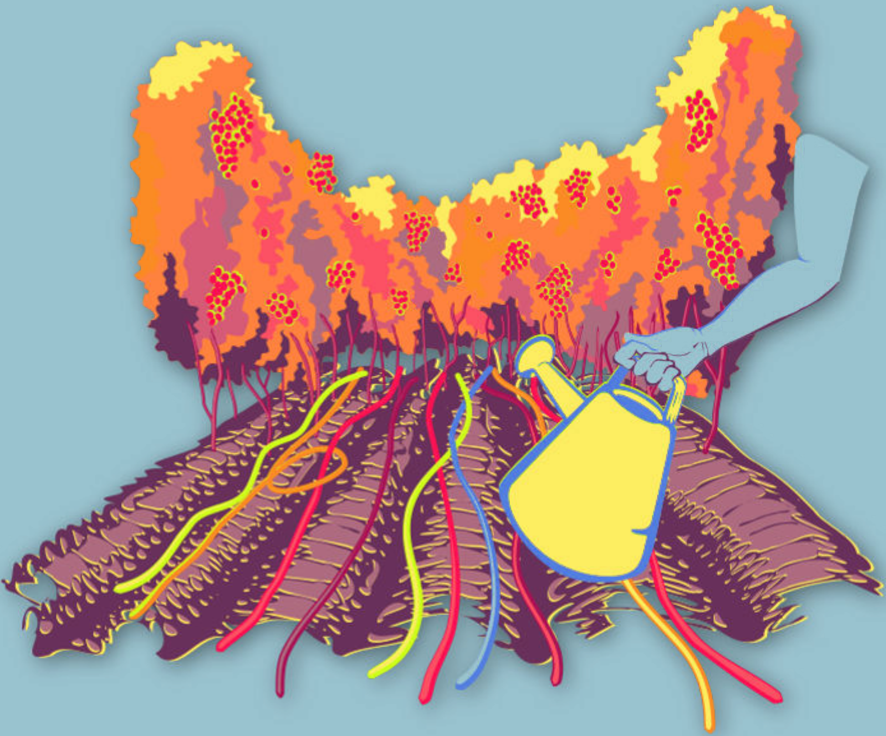
CYBERWOMEN



Planning ahead

Digital security plans and protocols: post-training replication

INSTITUTE FOR
WAR & PEACE REPORTING
IWPR

© 2019– Institute For War And Peace Reporting

https://iwpr.net/

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.

https://creativecommons.org/licenses/by-sa/4.0/deed.en

Contents

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/