**2.2 Rating Information Sensitivity**

**Intro:** Participants learn to assess the sensitivity of their information using a 3 level sensitivity framework (low risk, medium risk, high risk).

**Timing:** 30 minutes

**Equipment Needed:**

* Whiteboard or large sheets of paper and markers to list out participant’s contributions and take notes.
* Printed copies of the [Risk Assessment Preparation Worksheet: rating information sensitivity](http://www.google.com/url?q=https%3A%2F%2Fdocs.google.com%2Fdocument%2Fd%2F1HFZVtsvSdIW8pp_tstbg23aRN4iDYPvqjYzs1ROvbJ8%2Fedit).

**Content Outline and Main Topics:**

1. **Instruction/Exercise (30 mins):** Preparing for Risk Assessment: rating information sensitivity.
2. **Exercise (20 mins):** [Risk Assessment Preparation Worksheet: Rating Information Sensitivity](https://docs.google.com/document/d/1HFZVtsvSdIW8pp_tstbg23aRN4iDYPvqjYzs1ROvbJ8/edit).

**Objectives/Expected Outcomes:**

* Participants will catalogue the information they communicate or store on their mobiles, and rate it for sensitivity using the [Risk Assessment Preparation Worksheet: Rating Information Sensitivity](https://docs.google.com/document/d/1HFZVtsvSdIW8pp_tstbg23aRN4iDYPvqjYzs1ROvbJ8/edit).

**Additional Resources for Trainers and Participants:**

[Guide to Mobile Security Risk Assessment](http://mobileactive.org/risk-assessment)

[Mobile Security Risks: A Primer](http://www.mobileactive.org/howtos/mobile-security-risks)

<http://www.mobileactive.org/howtos/mobile-security-risks>

**Content**

**1. Instruction/Exercise (30 minutes):** Preparing for risk assessment: Rating information sensitivity.

A first step when conducting a risk assessment for an organizational security policy is to rate the sensitivity of various categories of information.

* What makes information sensitive?
  + There is no one static definition of sensitive information, nor is there one right way to manage information deemed sensitive.
  + As a general guideline, sensitive information, unlike public content, is i**nformation that will put you or your operation at risk if it is known by people other than yourself and your trusted colleagues.**
* A helpful breakdown: Three levels of sensitivity
  + **1. Low (public).** Public information can be freely distributed by you, your organization, and your supporters, without any risk to individuals or organizational operations. In communicating **public** information, you can send and receive this information without taking any precautions. (*Example: A public press release may fall in this category.*) Similarly, release of **low-risk** information may result in minimal risk to you, your colleagues, and your community, and your organization. With low-risk information, individuals and the organization can protect themselves from risks and absorb the impact. (*Example: A text message reminding people to vote on an election day might be low-risk, if there is low expectation of violence around polling places.*)
  + **2. Medium.** Release of medium-risk information may result in risk to you, your colleagues, your community, and your organization. In order for individuals to protect themselves against such risks, individuals and the organization may have to adjust behaviors and tactics. (*Example: A message informing people of an event at which you do not want people outside of your organization present -- such as reporters -- might be medium risk.*)
  + **3. High**. Release of high-risk information may result in risk to you, your colleagues, your community, and your organization. Individuals might face serious physical risk and personal loss that can not be remedied. The operations of the organization might be jeopardized, endangering the ability of the organization to continue operating. (*Example: A photo or video showing the faces of people who participated in an illegal action, or an action that places them at risk of violence, might be high-risk.*)
* Ask participants what categories of information they manage using mobile communications. Remember, this can include information communicated via voice, SMS, email, social networks, and media captured with mobiles. It can also include any information you store on your phone, including contact information, calendar appointments, records, and more.
* Using the [worksheet](https://docs.google.com/document/d/1HFZVtsvSdIW8pp_tstbg23aRN4iDYPvqjYzs1ROvbJ8/edit), assign public/low/medium/high levels of sensitivity to the categories of information communicated via mobiles, contributed by participants. Many will overlap more than one level of sensitivity. Help encourage a discussion that drills down and encourages participants to explain why some information falls into one category or another. Discuss how these sensitivity ratings may vary depending on the organization, nature of work, operating environment, or type of activity being conducted.

**Scenarios**: Try to pick scenarios that are relevant to the participants and their operational context and focus areas. Information is sensitive because of its role in a particular organization, project, or operation, which in turn takes place in a particular operational context.

For individuals, consider the sensitivity of the following basic information:

* Your address if you are (this first one is hypothetical, then it goes to each of the participants considering their actual situations):
  + A public figure.
  + An activist working in an open society, but may not want all your activities public.
  + An activist closely monitored society who is targeted for your work in journalism.
* Your personal calendar or schedule on your phone. How do participants feel about this given their personal situation?
* Your phone number?
* Your address book and contacts in your phone, right now?

Use more complex scenarios to map out all the possible pieces of information that pass through various channels on your phone (IM, voice, SMS, email, VOIP, social media, pics, videos). Try to take each scenario, work with the participants to think of all the possible forms of communications that would or could be used for each, and map them out on the board in a matrix, then assign sensitivity to them.

Here is an example.

|  |  |
| --- | --- |
| **Sensitivity Rating** | **Content** |
| Low | * Email with news clipping * A public meeting location * Text message telling people to vote in an election |
| Medium | * Pictures of law enforcement that result in your phone being confiscated during a protest. |
| High | * Email with report of HR violation by confidential source * A secret meeting location |

Scenarios:

* Journalists are covering a protest where news coverage not welcome. Although reporters are currently allowed to operate without harassment, there is concern that this may change.
* A non-violent activist group is planning a protest in a country where protests are technically legal, but the current government is in opposition to the group’s goals.
* A foreign activist is collecting reports of human rights violations while visiting a country that could be considered “closed.” A colleague is trying to put the activist in contact with a local person who wants to share a report. Map out the activist’s communications with the colleague (who is not in the same country but helping them remotely) and with the local contact.

**2. Risk Assessment Preparation Worksheet (20 minutes):** Rating information sensitivity.

Every participant or group of participants who will be developing a risk assessment should prepare their own copy of this [worksheet](https://docs.google.com/document/d/1HFZVtsvSdIW8pp_tstbg23aRN4iDYPvqjYzs1ROvbJ8/edit). As preparation, participants should itemize sensitive information for their work. This can be done during this section, or as homework.