**4.1 How to Assess Your Risks**

**Intro:** This session builds on earlier lessons to help participants assess risks they face by completing the Guide to Mobile Security Risk Assessment. The content is highly dependent on what has been covered previously. Trainers walk participants through the guide to help them better understand what elements make them uniquely identifiable as mobile phone users as well as to define, identify, and assess risks they may face.

**Timing:** Varies

* If you are using this module to introduce concepts that are new to many participants, we suggest identifying one example, preferably one shared or equally known by participants, to use in order to illustrate the process. The [Guide to Mobile Security Risk Assessment](http://mobileactive.org/risk-assessment) uses Asima’s mobile risks as an example, which could also be used for this exercise. Participants then repeat the process in Exercise 8, this time using their own project or organization. (**1.5-2 hours for this unit, 2-3 hours for Exercise 8)**
* Alternatively, you can choose to cover the concepts in this unit using ad-hoc example scenarios suggested by participants, then take any questions, saving the risk assessment worksheet until Exercise 8 where participants will put their assessment skills into practice by performing risk assessments and constructing security plans and protocols.**(1 hour for this unit, 2-3 hours for Exercise 8)**

**Equipment Needed:**

* Whiteboard or large sheets of paper and markers to outline instruction content and participant contributions, and to take notes.
* Have participants read the [Guide to Mobile Security Risk Assessment](http://mobileactive.org/risk-assessment)before the training; ask that they bring any questions they had about the guide to the training. You may want to print a few copies of the guide for participants to refer to during the session.
* If you are using a prepared scenario, prepare on slides or print out copies of the scenario and a completed risk assessment worksheet for that scenario.

**Content Outline and Main topics:**

1. **Introduction (5 minutes):** All risks are not the same. Impact x likelihood.
2. **Instruction (5 minutes):** Things to know about mobile risks.
3. **Exercise (10 minutes):** Identify the information you manage on your mobile, and classify it according to sensitivity.
4. **Instruction/Discussion (15 minutes):** Your risks depend on your operational environment.
5. **Instruction (10 minutes):** Categories of threats for mobiles.
6. **Instruction (15 minutes):** Thinking about mitigation.
7. **Instruction/Discussion (15 minutes):** Putting it all together - A system for assessing risks an choosing mitigation strategies.
8. **Exercise (20 minutes):** Risk assessment practice.

**Objectives/Expected Outcomes:**

* Participants are introduced to the concepts underlying risk assessment and security policy development: risk, vulnerability, likelihood, and impact.
* Participants practice cataloguing their mobile communications in terms of the sensitivity of the information involved.
* The role of operational environment in determining risk is reinforced.
* Participants practice conducting a systematic search for vulnerabilities and mitigation tactics.
* The concepts (risk, vulnerability, likelihood and impact) are put into use in group discussion around a basic risk assessment.

**Additional Trainer and Participant Resources:**

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

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

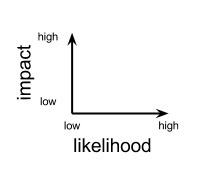
[APC’s Information and Communications Security Training Materials](http://www.itrainonline.org/itrainonline/mmtk/security.shtml#Information_security_planning)

[Frontline Defenders](http://www.frontlinedefenders.org/esecman)

**Content**

**1. Introduction (5 minutes):** All risks are not the same.

* Question to participants: What **risks** are you exposed to in your personal life? In your work? For example, your laptop being stolen, you being mugged, or the threat of arrest. Make a list together. At this stage, any kind of threat can be on the list
* What is the **impact** and **likelihood** of each of these risks? Draw a graph of impact versus likelihood (see below), and ask participants to classify risks accordingly.



**2. Instruction (5 minutes):** Things to know about mobile risks.

* *It is not possible to identify all risks, nor is it possible to eliminate all risks, particularly with mobile devices. Your goal should be to understand your risks and know how to mitigate as much risk as possible.*
* Remember that security assessment and risk mitigation are resource-intensive processes.
* You will become more confident at assessing and designing security practices with more practice, experience, and knowledge. As your confidence increases, you will find it easier to make quick changes in response to changes in your environment.
* Regardless of your level of experience, the risk assessment process involves requesting assistance from and collaboration with others, asking lots of questions, and doing your own research.
* It’s easy to ignore or reduce your focus or forget about security until something goes wrong. Realize that although you and/or your organization may feel like performing a risk assessment for your communications is unnecessary or not the best use of your time, an assessment and strategic planning is vital to your work, especially now that so much of what we do and communicate is done using online and mobile tools.
* The purpose of these trainings on assessment and planning is to help you formulate a realistic plan for yourself or your organization, as well as one that you can manage yourself.
* Realize that while we focus on mobiles, your information security policy should extend to online digital security and physical security. Security is interdependent and connected. For more information on how to incorporate physical security into assessment and planning, participants can to refer to [Frontline Defenders’ materials](http://www.google.com/url?q=http%3A%2F%2Fwww.frontlinedefenders.org%2Fesecman&sa=D&sntz=1&usg=AFQjCNHKvWBVds4sNHqC_pW0pJ7VZo2dCg).
* We’ll focus more on this in the planning section to follow, but keep in mind that for all situations, we suggest you first address easily-managed risks. Then, focus on more resource-intensive mitigation tactics for risks that carry the highest impact and probability of happening to you. The risk assessment will help us identify these, but remember that mitigation must be manageable for you.

**3. Exercise (10 minutes):** Identify the information you manage on your mobile, and classify it according to sensitivity.

This should also be a review from section 2.1 What Is Information Security For Mobiles? If you skipped this section, include more detail here.

* + **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 be low-risk or public information.*) Similarly, release of **low-risk** information may result in minimal risk to you, your colleagues, your community, and your organization. With low-risk information, individuals and organizations 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 organizations 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.*)

**4. Instruction/Discussion (15 minutes):** Your risks depend on your operational environment.

(Note: this is from Section 3.2 What’s your operational environment? If you have completed Section 3.2 in detail, structure this section here as a review)

Your operational environment can include *any* factors that allow or prevent you from operating to meet your individual or organizational goals, as well as what can define those goals.

Review the three main categories in your operational environment:

* Your work in the context of a given society and culture
  + Political and human rights
  + Reputation
  + Issue and controversy
* Technological vulnerabilities and threat
  + Mobile networks and devices
  + Availability and reliability of service
  + Policy and oversight
* Legality of your tactics and tools
* Are the tactics you are using considered legal where you are working?
* Are the security tools that you are using legal or illegal where you are working?

**5. Instruction (10 minutes):** Categories of threats for mobiles.

Many different types of risks exist, and you may only experience a few. When conducting a security assessment, it is good to think broadly about risk. The categories below can be used as a checklist for different kinds of risk to mobile communications.

|  |  |
| --- | --- |
| **Risk** | **Description** |
| Listening | A call can be listened to, or transmitted data can be read. |
| Modifying | Primarily a threat for data transmissions. The transmitted data can be modified. |
| Spoofing | A threat when the authenticity of the user is not guaranteed. |
| Identifying | The user identity and/or location is revealed. |
| Interrupting | Connectivity to the network is disrupted. |

**6. Instruction (15 minutes):** Thinking about mitigation actions.

In this Section (4.1), we introduced different categories for mitigating action. These can also be used as a checklist to help you search for ways to mitigate a risk.

|  |  |
| --- | --- |
| **You may be able to mitigate a risk by:** | **Example** |
| Changing your behavior | Not leaving your phone unattended. |
| Using a security tool | A phone feature (such as setting a PIN or password) OR an app (such as encrypted SMS). |
| Switching to an alternative mode of communication | Encrypted email or voice, instead of SMS. |
| Abstaining from a particular activity | Not taking a phone with you to a sensitive meeting you don’t want recorded or overheard. |

**7. Instruction/Discussion (15 minutes):** Putting it all together. A system for assessing risks and choosing mitigation strategies.

In the context of security, **risk** has a particular meaning.

* A **threat** is anything that has the potential to cause harm.
* **Risk** is the **likelihood** that a **threat** with a particular **impact** will occur that causes harm or loss.
* A **vulnerability** is a weakness that could be used to endanger or cause harm.

So, what creates a **risk** for you? The **likelihood** that a **threat** with severe **impact** will use a **vulnerability** to cause you harm.

Take the threats mentioned by participants in the last section, and draw up a table to illustrate risk in terms of vulnerability. Use a simple scenario that can be described in one sentence and easily understood by all participants. In the next exercise, we will progress to more complex and personal scenarios, and participants will work on their own.

**Example: Using your mobile phone to check Facebook on the subway in NYC.**

|  |  |  |
| --- | --- | --- |
| **Risk** | **Impact (likelihood)** | **Mitigation** |
| Physical surveillance - someone sees you enter your information | Someone sees you enter your account details, and steals them (low) | Cover your screen, be aware of who is around you in public places |
| Someone takes your device and accesses your information | Unauthorized access to the data on your phone, contacts, messages, calender, online accounts (low) | Password protect your device, using strong passwords, install InTheClear or another backup/remote wipe app |
| Lost/dropped/stolen device | You need to spend money to buy a new device (low) | Be aware of where your phone is, leave it at home when going to a risky situation |
| Service outage no network | You can’t get online (high - it’s a subway!) | Don’t rely on your mobile alone, be aware that the network can go down at any time. |

**8. Exercise (20 minutes):** Risk assessment practice.

If you are walking participants through a risk assessment process using a predefined scenario, you can prepare a sample assessment in advance using the assessment [worksheet](https://docs.google.com/leaf?id=0B0j5_3vVWZ8tNGJiZWQzMWItMDM3Ny00ZDRmLWFiMTMtNzk2MzkyNzUwNTg5&sort=name&layout=list&num=50&ndplr=1&pli=1). Otherwise, draw out the columns of the worksheet on a large sheet of paper or whiteboard, and run through a basic scenario of participants’ choosing. The objective here is to start **using the vocabulary and concepts** introduced in this section, together with the **content** (vulnerabilities and mitigating actions) participants have been exposed to in previous sections.

Using the tools you’ve learnt about so far, consider:

* How you communicate and store sensitive information via your mobile phone.
* All parties involved (such as the sender and receiver of data) and their security needs and policies.
* The purpose and content of the communication. How sensitive is the information?
* Your operational environment.
* The risks you may face.
* Ideas about possible mitigating actions.

Once you are done, revisit the purpose and goal of your organization, campaign, or event. Be clear on the goal(s) of your proposed action, and how it will affect the work of your organization. This will help sharpen your thinking when making difficult decisions on risk.

* Sometimes you will need to decide whether or not that particular action or piece of (high-risk) information is critical to your goal.
* It is inadvisable to take certain risks; sometimes individuals take risks that do not benefit them as much as expected. The more of these that you can eliminate beforehand, the safer your activities will be.