



# Threat modeling guide

How to identify digital risks in international development projects



# Threat modeling guide

How to identify digital risks  
in international development projects



---

## Imprint

### PUBLISHER

Deutsche Welle  
53110 Bonn  
Germany

### RESPONSIBLE

Carsten von Nahmen

### AUTHOR

Daniel Moßbrucker

### CONCEPT

Julius Endert  
Lina Hartweg  
Daniel Moßbrucker

### EDITORS

Hannah Correll  
Tobias Hübers

### COORDINATION

Bahia Albrecht  
Eira Martens-Edwards

### DESIGN

Nilab Amir

### ILLUSTRATION

Marc Löricke

### PUBLISHED

September 2020

© DW Akademie



## Contents

<b>Executive summary</b>	<b>06</b>
<b>Why is digital security crucial for your work?</b>	<b>08</b>
Your data makes you an interesting target	09
Why is it up to you, not the IT department?	09
Protecting your daily work	09
<b>How do you use this guide?</b>	<b>10</b>
<b>What is threat modeling?</b>	<b>12</b>
Risk assessment	13
Four threat dimensions to consider	13
Applying threat modeling to your work	14
Question zero: Knowing your environment	15
<b>Threat modeling, step by step</b>	<b>16</b>
Question zero	17
General advice: Include a threat model in your project plan	17
Going deeper: Explore your project	18
Question 1: What do we want to protect?	22
Question 2: Who are our attackers?	25
How external attackers are connected	26
How data is exchanged amongst different entities	27
The human factor and internal resistances	29
Question 3: Are our attackers able to succeed?	32
Question 4: How likely is it that our attackers will succeed?	40
<b>Outcome: Towards your own digital security concept</b>	<b>44</b>
<b>Annex</b>	<b>48</b>

# Executive summary

Digital security is crucial for international development projects. In the interviews and research conducted for this guide, members of civil society from all over the world shared multiple examples in which they lost critical data, were harassed on social media, were under surveillance by a state-driven actor or had to hand over digital devices to the police. Threats come in many forms: Sometimes employees are not well trained on how to use computers and accidentally lose data, othertimes powerful attackers go after activists and their supporters.

Although the space for human rights defenders is shrinking and digital security incidents happen, the awareness in many organizations is still relatively limited. There are numerous reasons for this. First and foremost, employees are not aware of certain risks or how to prevent them. Surveillance is usually concealed: You do not realize that your phone has been compromised, that hackers have stolen your data or that you have provided your email password to a phishing site until it is too late and your attacker has the information.

This is the dilemma: A security concept needs resources, like time and money, but you only know it wasn't enough once it has failed. We don't see the direct risk of surveillance in our lives, so, a lot of people think that they do not have to worry about it at all. Many real-life cases documented in this report prove that this is a dangerous belief.

So how should we approach digital security? Threat modeling can help.

Threat modeling is a formalized, IT-based risk assessment process. It consists of defining objects to protect and identifying attackers that may want to compromise these assets. The result of the process is a project-specific threat model.

This how-to guide was specifically designed for project managers that work for international development organizations and cooperate at the project level with NGOs in developing countries, but it can also apply to other sectors. In international development, threat modeling assessments cannot solely be done by IT specialists because the regional and country-specific context of a project is of particular relevance. On the contrary, project managers should go through threat modeling themselves based on their situational needs in order to provide guidelines for anyone involved in improving their project's digital security. However, this does not mean it is the work and responsibility of the project manager alone.

The structured analysis asks four key questions about digital security risks. Each section of this guide will explore another dimension of digital security—assets, attackers, risks and likelihood — and address these key questions:

- **What do I want to protect?**
- **Who are my attackers?**
- **Is my attacker able to succeed?**
- **How likely is it that my attacker will succeed?**

Threat modeling consists of two types of assessments: Firstly, an analysis of the project's environment (questions one and two). Secondly, an estimation of the likelihood that potential attacks will really happen (questions three and four).

To prepare for threat modeling, we have added a "question zero" for project managers: Who are we and what do we do? This helps to establish a clear understanding of the entire project, with all of its workflows and challenges that employees face in their day-to-day work environment.

A threat model is the basis for a digital security concept that should be developed along with IT experts so that your concept is both technically sound and practically enforceable. Having a clearly defined list of assets and their vulnerability empowers employees to protect them with appropriate countermeasures, and educates them on risks. This will increase the efficacy of a security concept in practice.

# Why is digital security crucial for your work?





Think you have got nothing to hide? Well, if you are responsible for the safety of your team members, partner organizations or activists and journalists you collaborate with, this can be a dangerous attitude. This how-to guide is designed for project managers that work for development organizations and cooperate on a project level with NGOs in developing countries, but also applies to other project models. We aim to help you to identify digital threats, an essential step in making a digital security concept that is effective and meets your needs in practice.

## Your data makes you an interesting target

You probably work with your project's internal research papers and guest lists for events with the names or contact information of attendees and rather sensitive partners on a daily basis and process it digitally. If this data ends up in the wrong hands, it could put people in real danger. As a project manager in a digital world, it's crucial to know effective general countermeasures against digital threats.

We cannot just accept digital risks as unavoidable and not take action. Doing nothing can have serious consequences. In Pakistan the NGO Bytes for All documented many cases of phishing attacks against Pakistani members of civil society. Phishing is a rather old but powerful tactic: In the Pakistani cases, clicking on a malicious link or attachment in emails, for example, led to computers and smartphones becoming infected with the malware StealthAgent. This software means an attacker can, for example: intercept phone calls, steal photos and search emails.

An employee of a local NGO in the Democratic Republic of Congo shared the following story during a research interview for this report: *"I was recently working on our annual report to be submitted to the Board and then to a partner. Some messages popped up on the computer asking me to download an anti-virus (software) to keep my computer safe. I followed a few steps, which led my computer to suddenly shutdown. I don't know what happened, but I could not find my documents anymore, losing everything that I had worked on for a few months. This incident had an impact on my work because I was blamed by my manager for not being able to meet the deadline."*

This common scenario demonstrates the danger of digital threats, which members of civil society and their supporters often face. Even unsophisticated attacks are effective if people are unaware of risks and hacking tactics, especially ones that are undetectable, meaning a victim has no way of knowing they are being spied on or were targeted.

## Why is it up to you, not the IT department?

Especially in international development, a project's regional context and situational needs matter a lot. Stakeholders who are not involved in the project's daily operations might suggest a solution that is secure but impractical or does not meet your specific needs. The technology might only be safe in theory. If you develop your own threat model, it is more likely to be applicable to your project in reality. Also, the threat model will serve as a foundation for others to support you with fitting solutions that you can really use.

### Example: Theoretically safe solutions



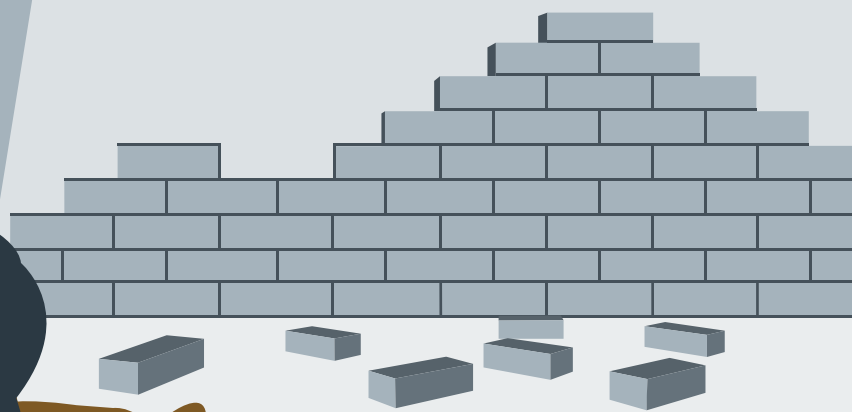
You worry government spies may physically break into your office in a partner country and steal sensitive data from computers. Simple tips from experts or your IT department might be to encrypt the hard drive and use a secure password on the computer. But how will they know that such a risk exists for your project? And how can the IT department know if their suggestions match your team's computer skills?

What if their solution is only safe in theory? Someone might encrypt a hard drive, forget the password and not be able to access the data anymore, or not even encrypt it because the program is too complicated. A threat model that you create will outline risks based on your team's actual computer usage and will guide your IT department—or other experts—so they can give you better tips, like an additional plan to save passwords securely in a backup. That is why a threat model is, and should be, your job as a project manager. ■




## Protecting your daily work

How should you, as a project manager with little tech knowledge, be able to protect yourself against such sophisticated threats? It should not be your responsibility alone, but it is your task to identify specific needs by analyzing your daily work and then address these needs with the support of experts. The IT-based threat modeling we present to you here will show you how.

How do you use  
this guide?



*This guide will help you answer the most challenging question: How do I create a digital security concept? Step by step, you will learn to go through the “threat modeling” process on your own.*

In the  dark blue boxes, we will share materials you can use to assess all needs and risks with your team. In the  light blue boxes, we highlight the essentials of every step. Case studies will demonstrate how threat modeling works in practice (see the  grey boxes, “Case study”). These are useful for making the process more tangible and can help you discover the specifics of your own project, but you can also skip the case study. For every chapter, we have also provided real-life examples, material for further reading and concrete “how-to” recommendations. These are signposted throughout the guide with the symbols you can see on the right hand side of this page.

After a general introduction to digital security, the five phases of creating your own threat model are presented. The end goal is to have a customized threat model for your project, which helps IT specialists to build a system based on your practical needs, as well as secure tools for your safety.

Now you have two options for how to proceed. The following chapter provides more information about the concept of threat modeling. We recommend this chapter for project managers intending to hold a workshop based on this guide with their team. However, you can also jump to the step-by-step guide to making your own threat model, starting with the chapter on “question zero”.



Exercise



Summary



Casestudy



Example



Further reading



How-to

## Threat check

---

Threat check is an online application developed by DW Akademie that aims to help project managers in international development organizations and their local partners to create a digital security plan. The interactive tool covers different topics you can choose from, such as account security, travel security and online harassment, among others.

Threat check generates customized digital security tips on the selected topic for your individual project or organization:  
[➔ \[akademie.dw.com/threatcheck\]\(https://akademie.dw.com/threatcheck\)](https://akademie.dw.com/threatcheck)

---

# What is threat modeling?



Threat modeling is something we do numerous times every day without giving it a name. This chapter explains the general idea and process of threat modeling.

### Risk assessment

IT-based threat modeling formalizes the process of risk assessment, which human beings do every day in nearly every situation. It is always about both defining your assets and identifying your attackers who might be willing to compromise these protected objects. These two assessments are matched to see what the most likely threats are.

likelihood of a successful attack (robbery, sexual assault, violence). Based on this analysis, you can make a decision: Is it safe to walk alone through the park, is it enough to take a flashlight with you or do you pay for a taxi to completely avoid the park? ■

Threat modeling gives you a list of priorities for your security concept. You won't have the solution implemented directly after modeling the threats, but you will know where to start. Colleagues and IT specialists can then help you with the implementation.

### Four threat dimensions to consider

As the example of walking in the park demonstrated, threat modeling consists of four phases.

#### Example: Walking through a park



You want to visit a friend who lives nearby, but you have to pass through a park without streetlights and some areas have no cellphone service.

You automatically start to analyze the situation (the route without light and phone connection), try to identify potential attackers (pickpockets, sexual or violent offenders), decide what you need to protect (your physical safety and personal belongings) and make an assessment of the

- Protection: What do I want to protect?
- Attacker: Who are my attackers?
- Risk: Is my attacker able to succeed?
- Likelihood: How likely is it that my attacker will succeed?
- Every phase analyzes a different dimension relevant to your IT security concept.

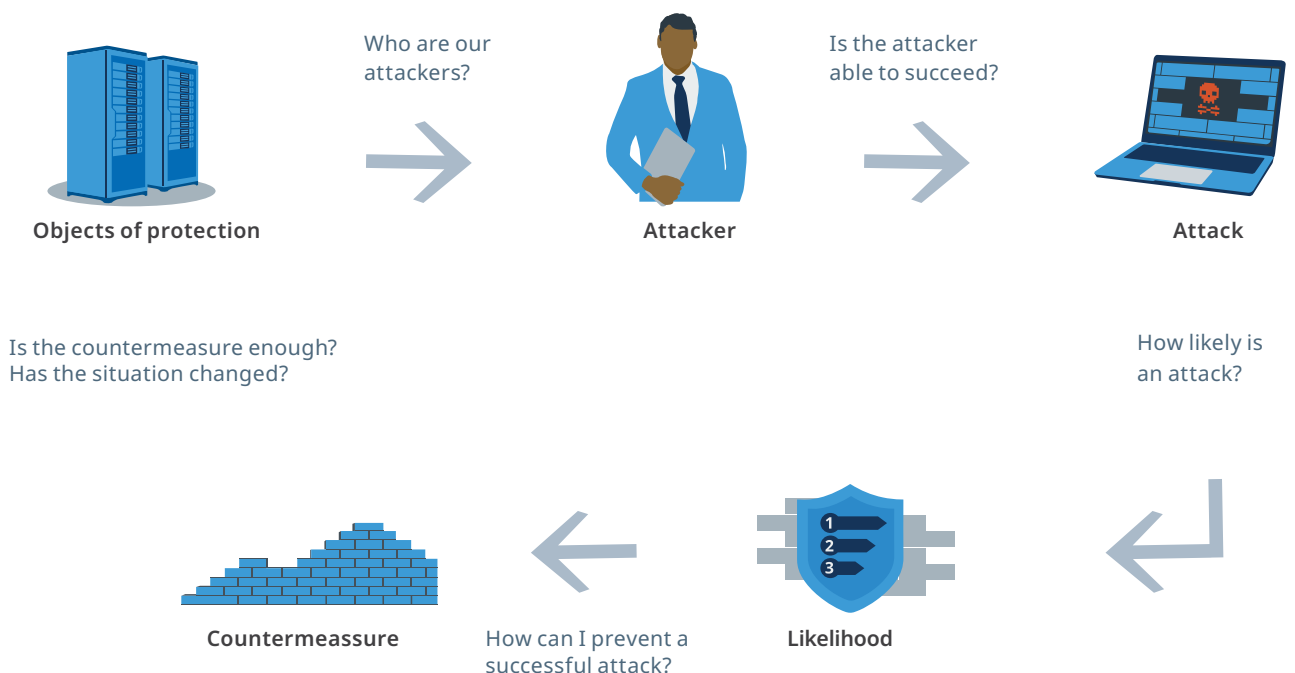


Diagram 1 The process of threat modeling

### Exercise 1: Discussing threat scenarios



If you want to practice thinking through threat scenarios, a group exercise is helpful. We provide four scenarios in the annex. Split your team into groups.

Each group gets a scenario and has to discuss how they would deal with the threat. After around eight minutes, the group has to share what they discussed and how the four dimensions — **assets** (objects you want to protect), **attackers**, **risk posed by attackers**, and **likelihood of attacks**—influenced their final decision. ■

### Applying threat modeling to your work

Let’s try to apply this four-phase approach to your daily work. A common challenge in daily operations is managing data that multiple employees have to use. Your project might partner with an organization that uses different IT systems than yours. With no common server to store your data, a commercial cloud-based option could be a smart solution. You might ask, “Is that safe?” It’s hard to answer such a broad question, but the four dimensions above can help to make it specific.

- **Protection:** What you want to protect is clear: the data stored in the cloud.
- **Attacker:** Your attackers are also obvious: cyber criminals looking for banking information to drain your accounts, and the national government of your project’s country, because

your project is critical of leading state officials. Consider so-called “internal vulnerability”, which could be your own teammates. Maybe they will unknowingly “help” your attackers access your data because they aren’t careful when using the cloud.

- **Risk:** Will your attackers succeed? This question is challenging because it requires you to know what their capabilities are, but that actually is not as hard as you might think. As you will learn, some groups of attackers tend to use similar hacking tactics. In our example, we assume a successful attack to be highly likely since it is theoretically possible and attackers have an interest in your data in the cloud. Any attackers can try to hack your accounts and a government might also have lawful ways to obtain data from a commercial cloud provider. “Internal vulnerability” in both the funding and partner organizations might put your data at risk since their understanding of cloud security is low.

After answering a few questions, you will begin to see potential threats. Maybe there aren’t attackers interested in specific assets, or a successful attack would not cause any serious harm. If that’s the case, you can focus on more pressing issues.

- **Likelihood:** This question is the most crucial, and often the most challenging one, since it is hard to estimate the likelihood of these threats. In this guide, you will learn sim-

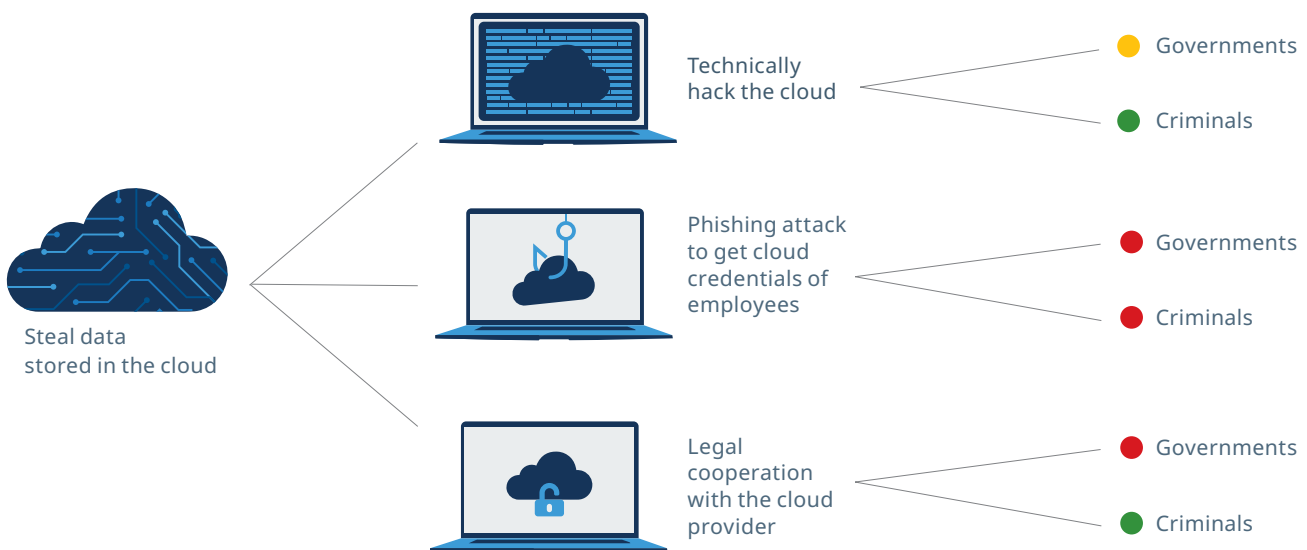


Diagram 2 Example of a threat scenario for working with a cloud. | high risk ● moderate risk ● low risk ●

ple strategies to estimate threats. We also have a list of resources in **question 4**, so you can consult experts with deeper technical knowledge.

As for cloud-based data management, several scenarios are possible. Both criminals and the government might use social engineering tactics on your colleagues to gain access to the cloud by sending phishing emails to steal login data for the cloud.

## Question zero: Knowing your environment

We have added a step to help prepare you for this project assessment: question zero. As the following diagram demonstrates, there is actually a question to consider before you begin the threat modeling assessment: In order to decide what to protect, you have to know your digital environment well. In our case study, that means the project manager knows there is a need for a cloud and that employees are struggling with existing solutions because they don't meet their needs. "Question zero" can be simple questions such as:

- Who are we?
- What does our project entail?
- What are our needs?

Another important step for project managers is mapping the entire project to get a complete overview of all the workflows and needs for the colleagues. This will be the foundation for the threat model. We'll explain how to do project mapping in the next chapter.

Diagram No. 3 shows the entire process of threat modeling. Your job is to answer the questions zero to four. The result of the threat modeling process is a customized threat model. With the assistance of IT specialists and consultants, you can go through the specific threats from your model and find a countermeasure for each one. This way your project-specific security concept will address your project's risks and not some generic, theoretical risks.

### Further Reading: Information on Threat Modeling for Non-Specialists



Reporters Without Borders: Interactive Threat Modeling Tool for Journalists and Activists.  
[➔ helpdesk.rsf.org/training/your-threat-model](https://helpdesk.rsf.org/training/your-threat-model)

Electronic Frontier Foundation: Journalist on the move? How to stay safe online anywhere without sacrificing access to information.  
[➔ ssd EFF.org/en/glossary/threat-model](https://ssd EFF.org/en/glossary/threat-model)

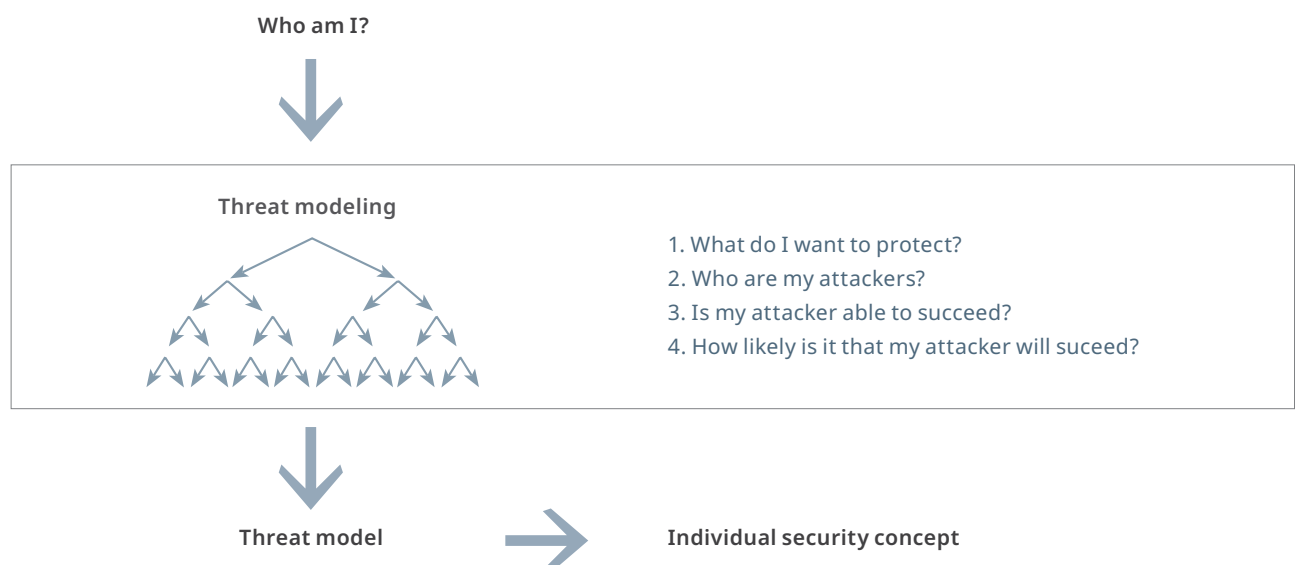


Diagram 3 *Digital security on the basis of a threat model*

# Threat modeling, step by step





*In this chapter you will learn how to create a customized threat model for your project.*

The next five sections will show you how to make a threat model. Prepare by assessing your project using “question zero” to get a summary of all project workflows. Then you will define all assets to protect within your project, determine attackers that pose threats and then match attackers to the assets they may target. Finally you will estimate the likelihood of each threat scenario so you can prioritize them. A case study will demonstrate each step as it is introduced.

### Case study: Defending freedom of expression



You are a project manager in a European international development organization that is mostly funded by European governments at the project level. The aim of the organization is to promote freedom of expression, focusing on strategic litigation. It identifies cases in developing countries where an individual's freedom of expression has been limited, to challenge them in court and call for more democratic legislation in the country. Thanks to new funding, you will manage a three-year project in a developing country. You want to cooperate with a longstanding local NGO. ■



*Before you can identify assets and attackers, you need to get to know your project better. This is an extra question to prepare you to answer the four threat modeling questions. You should consider your project's digital security from the initial planning stages.*

### General advice: Include a threat model in your project plan

Your project might be too far along for a threat model, but as a general rule: It is crucial to start thinking about digital security as early as possible—preferably in the first stage of the project planning. A digital security concept will work better and will be easier to implement if it is an inherent part of the project.

Threat modeling helps to decide what resources you need (devices, software, staff, consulting, time, etc.). You should estimate time and financial resources for this threat modeling process. Ideally the resulting workflow assessment will be a living document that you update every three to six months. Do this to add on any needs you left out of the threat model or digital security concept.

## Going deeper: Explore your project

Before you start the process of threat modeling, it is crucial to have an in-depth understanding of your project and its' (assumed) workflows. So here you will break down the general question of "Who are we?" by asking questions such as:

- What workflows exist in the project?
- Which employees are involved in the workflows and how?
- Which information needs to be protected to guarantee the safety of employees?

### Step 1: Assess all workflows



In the process of project planning, you assess all expected workflows. Try writing them out in a table with all involved teammates and related assets. It is important to be very specific, especially in listing digital, technological tools. Be sure all tools are listed next to each workflow.

### How it's done



To identify all workflows, think through a typical week and write down every workflow, meeting, travel and kind of communication that takes place. You—and one or two colleagues with different roles in the project—can observe your own behavior for a day or two, noting each workflow. Ideally, the entire team would do this as a group.

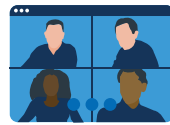
How detailed should it be? In general, more detail is better. When looking at communication, just mentioning "communication between two employees" is too broad. Try not to think technically and instead note behaviors and be specific: Do you use landlines for phone calls, chat apps like WhatsApp or email? Include the mode of transportation—by bike, car, public transport or airplane.

You can do this in a table containing the workflows, involved teammates and related assets. Remember to focus on digital technology. We suggest you write down the names of the services you use in each workflow. Include the information that is processed in a workflow in the next column over from the assets. For example, for a weekly team conference, you would list that status updates are shared along with information about sources and ongoing project strategies.

This list of information is important for a later phase of the threat model where you will classify information based on the degree of confidentiality. In order to make that step easier, classify information in this stage. We suggest using these four categories, indicated in your table using numbers:



**Public information:** is accessible to everyone inside and outside of the organization, e.g. texts on the website, used by employees in interviews or used in the organization's reports—classify with 0 in the table.



**Internal information:** is not accessible to the public, only for (certain) staff members. However, disclosure would not have dramatic consequences for the organizations. Examples could be travel information for employees attending a public event, working hours of team members, communication on the planning of public events or contracts with external companies, such as for the cleaning of the office—classify with 1 in the table.



**Confidential information:** is not accessible to the public and only to a few staff members. Disclosure would have a significant impact on the work of the organization, but not necessarily on the safety of its people. For example, drafts of research reports that will be disclosed soon or internal summaries of closed meetings with politicians on advocacy—classify with 2 in the table.



**Highly confidential information:** is not accessible to the public and only to a few staff members. Disclosure would have a significant impact on the work of the organization, and on the safety of its people. For example, the identity of sources for reports or research strategies for potential attackers like corporations—classify with 3 in the table.

It should be noted that these categories are meant to help you get a feel for the level of the information's confidentiality. Maybe travel information would count as internal information, but a meeting with a source is then, of course, highly confidential. Here we are talking about an assumed level of "typical" confidentiality, but your threat model requires your insight and should be flexible enough to adapt to your context, should exceptional situations arise. *See table 1*

### Exercise 2: Think-pair-share to identify workflows



A good method to collect as much knowledge and experience as possible, is the "Think-Pair-Share" method. The idea is simple: First everybody thinks about a question on their own.

Workflow	Employees	Object of protection	Shared information
Weekly team conference, remote dial-in via Skype	All team members	Content of team conference via Skype or within the conference room	Project status updates (2), research strategies (3), sources for research (3), ...
Team communication for various reasons, via email	All team members	Team's entire internal email communication	Project status updates (2), research strategies (3), PR plans (1), duty roster (1), passwords for social media accounts (3), ...
Publishing project-related messages on social media	Employee in charge of PR	Social media account credentials for Facebook, Twitter and Instagram	Project-related information for the purpose of PR (0)
Research on the internet about potential violations of freedom of expression	Research unit	Internet history from research, identity of potential sources	(Sensitive) project-related research information (3), identity of sources (3), ...

0) public information, 1) internal information, 2) confidential information, 3) highly confidential information

**Table 1** Typical workflow assessment with classification of information

Secondly, everybody exchanges their thoughts with a partner, and finally, everything is presented to the group.

As a project manager, you may use this method to summarize all workflows of your project. First, everybody gets five minutes to list workflows on their own, then five minutes to share their results with a partner, and 25 minutes to collect all results in a group discussion. We've provided a blank workflow chart with guiding questions in the annex. During the group discussion, add each workflow to a table everyone can see. ■

Even though your goal is developing a digital security concept, a smart first step is a broad assessment of all project-related assets. Don't forget "analog" items that need to be secure. Sometimes digital technology feels like it exists separately from the physical world, but attackers attack victims where they are most vulnerable. That can be an "analog loop-hole" in your security concept, making all your advanced digital security measures useless. For example, having strong encryption for finance data stored on your computer will not help you if you have paper copies of it in your office. Keep in mind, the most likely threat to your office may be burglary.

### Exercise 3: Count the analog risks

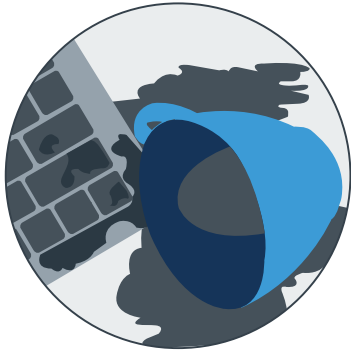


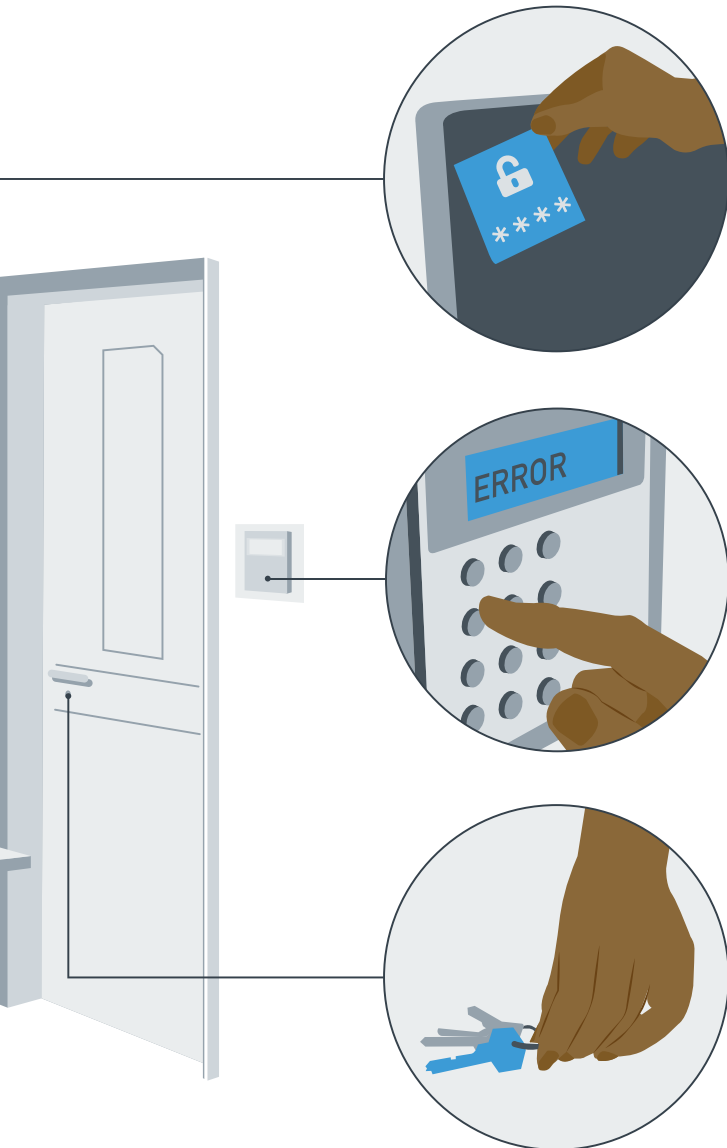
In a group exercise, you and your team compete to search the office and find the most dangerous "analog risks" pictured on the next page. Take ten minutes to tally up as many as possible. We'll get you started with the most common ones: an alarm that doesn't work, door lock that doesn't work, lost keys, open windows in crucial areas, passwords written down on paper and left accessible to anyone, open bottles on a table next to sensitive devices or documents, cabinets that cannot be locked, documents tossed away without being shredded... ■

### Step 2: Get information about organizational guidelines and restrictions



Do some research on implementing security concepts sooner rather than later. This makes it more likely that you can fully implement your concept, so be sure to find out about all internal or budget restrictions.





### How it's done



If organizational guidelines or other restrictions exist, they are probably documented somewhere, or your bosses may have information on them. Although they are not directly necessary for the threat modeling process, they might answer questions, for example about your maximum budget for new technology or software licenses. Reading existing guidelines could help you get a better picture of “typical projects”, too. Be sure to do this research while you go through threat modeling.

Write down all the answers you come up with as you go through these helpful questions:

- Which responsibilities and liabilities exist in your organization and potential partner organizations?
- Which guidelines for digital security, for example communication plans or data protection guidelines, are already in place?
- What budget do you need—or have—to conduct a threat modeling process?
- What budget do you need—or have—to implement a digital security concept?

### Case study: Identifying multiple workflows and involved partners



Since the project is still in the planning phase, you cannot monitor existing workflows, but have to make an estimation. The main task of the project is to identify significant violations of freedom of expression in the implementation country, file a case and publicize it. Therefore, researchers at the local NGO monitor the news and social media to find potential violations. They also communicate with victims and other sources who provide information about human rights violations in the country. The local NGO cooperates with an external, local law firm that writes the filings for cases, and with a PR agency that handles campaigning and media relations. Your organization consults with a local NGO that has years of experience in strategic litigation for freedom of expression. It also plays a role in picking which potential cases will be brought to court, and it controls the project budget. ■



## What do we want to protect?

*This phase of threat modeling takes the workflow assessment further, adding practical detail with a technical perspective. You will learn how to apply a technical perspective to workflows, making your assessment more helpful.*

The first question of the basic threat modeling process asks which of the objects of protection (assets) you want to protect. The table of workflows you've created to answer question zero will help you focus on information and workflows that are the most crucial to the success of your project. Be detailed and accurate in this step. Broad terms like "our life" or "our project" may be accurate, but are too general to find a fitting countermeasure—especially with regard to a digital security concept. This step is again about breaking a broad asset into segments that can be protected through your digital security concept.

### Step 3: Define the objects and workflows you want to protect



On the basis of the mapping of project-related workflows, you should now analyze the objects you would like to protect. If you did a chart with all workflows, nearly all of these objects can be found in the third column "workflow". This list includes

everything that seems to be protectable and is not limited to digital communication and technology, but also incorporates "analog" risks. You should also add a column to list the information that is transferred in these workflows. This will help you later to classify information from "public" to "highly confidential".

### How it's done



You will soon see there is a lot of overlap in your chart. For example, you may have listed different weekly Skype calls, but the object of protection is always the same: a Skype conversation. Try starting with a separate chart to list all of your project's assets to reduce repetition. Careful: Do not delete the column of shared information, but merge cells with the same service or device listed in them. *See table 2*

In the next step, group all your assets in broader categories to determine the value of protecting each asset. We conducted interviews with project managers working in international development, individually and as a group; according to their feedback, the most commonly mentioned assets to protect are:



**Physical integrity of the office:** An office holds nearly all of an organization’s information that needs to be protected, either analog (on paper) or digitally (on computers). Protecting the integrity of the office starts with stopping attackers from gaining physical access—legally or illegally—to your office.



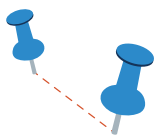
**Physical safety and freedom of employees:** People’s work sometimes puts them in danger. Attacks can be physical and in public spaces, or a country’s authorities can use legal tactics to restrict civil liberties.



**Integrity of IT:** As the IT infrastructure of an organization or a project holds a huge amount—if not all—of the information that must be protected. The integrity of these systems is crucial. Guard against attackers finding unauthorized ways to access servers, computers or smartphones or other protected information. They might log in as an administrator to the organization’s network or exploit vulnerabilities in the code of software you use.



**Travel safety:** International development employees travel a lot and border crossing can be hazardous. Employees rely on external infrastructure such as the airports’ WiFi or can be legally forced by border agents to reveal passwords for their devices and accounts.



**Location data and travel plans:** Data on where people are or will be travelling reveals a lot about their professional life, for example what they are probably researching or who they will meet. Movement profiles are often sensitive and require protection.



**Internal communication:** The communication of the team is a crucial asset to protect. Most of the in-person conversations, calls, chats or emails, contain a lot of sensitive information. The team is made up of all members of the organization and anyone who is consistently involved in a project, for example employees of partner NGOs and external service providers.



**External communication with partners and sources:** Not all communication can be protected. For example, if an organization has to communicate with government officials via phone, sensitive information about the government will probably not be discussed. Sometimes there will be confidential conversations with informants or trusted contacts that are not part of the core project team. Such communication is often spontaneous, but also needs to be protected.



**Identity of sources or undercover employees:** Not only the content of communication may be necessary to protect, but also the identities of those communicating. Not only the “What?” of a conversation may matter, but also the “Who?” with “Whom?” and sometimes even the “Where?” and “When?”. This “metadata” is especially important to protect if people’s anonymity has to be guaranteed. In the case of email, metadata includes the sender and recipients’ addresses, as well as a timestamp and subject line. If this is something you have to protect, you should list it separately from the contents of an email, as it would have to be technologically protected in a different way.



**Online account credentials:** With access to online accounts, attackers can access a lot of information. Most vulnerable are often accounts of email providers, social media, cloud services and online shopping platforms. Login credentials such as usernames and passwords should be protected.



**Personal and bank details processed within the project:** During a project, personal data like names, addresses and contact details may be processed. They need to be protected against unauthorized access and illegal use, also because of data protection laws. Large amounts of money are processed within a project; to guard against financial harm and corruption, bank details and especially credentials have to be protected.

Category	No.	Workflow	Employees	Object of protection	Shared information
Internal communication	1	Weekly team conference, remote participation possible via Skype	All team members	Team conference call content via Skype and within the conference room	Project status updates (2), research strategies (3), sources for research (3), ...
Internal communication	2	International calls with partner organizations abroad	Research unit, executive director, partner organizations	Content of call via Skype	Project status updates (2), research strategies (3), budget information (1), administrative information (1), travel planning (1), ...
<div style="display: flex; justify-content: center; align-items: center; gap: 20px;"> <span>↓</span> <span>Reduced to</span> <span>↓</span> </div>					
Internal communication	1	Various communications via Skype	All team members, partner organizations	Content of call via Skype	Project status updates (2), research strategies (3), sources for research (3), budget information (1), administrative information (1), travel planning (1), ...

0) public information, 1) internal information, 2) confidential information, 3) highly confidential information

**Table 2** Reducing workflows after the general workflow assessment

At this stage you do not have to rank these assets in terms of priority. You will do that in question three. List everything that you think should be protected, even if you already know that there will be not enough time or money for it.

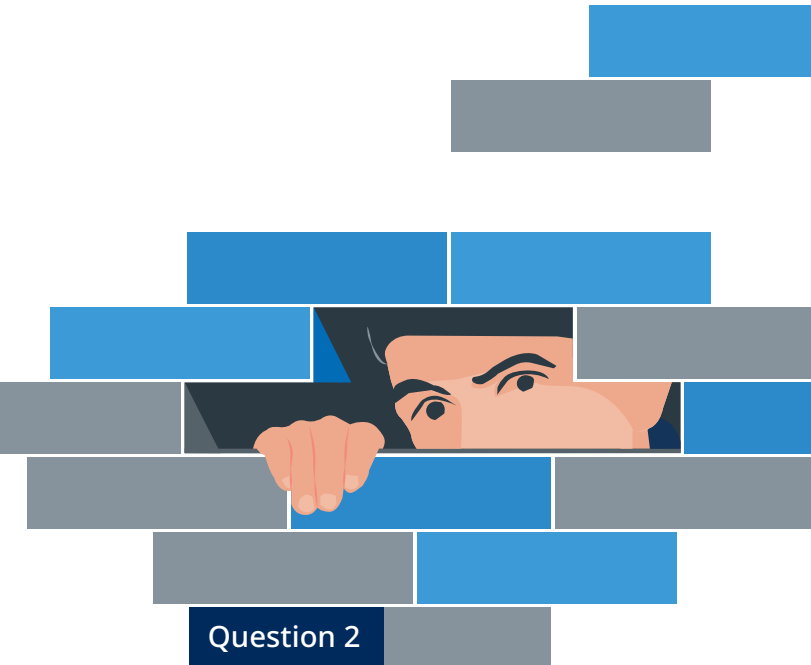
### Case study: Protecting the success of your legal battle



The object you have to protect the most within the project is the success of your legal cases, and all the employees and workflows that contribute to their success. You realize that communication within the team and communication with external service providers, like a law firm and a PR agency, have to be strongly guarded. During calls and email exchanges, sensitive information about the cases and sources are exchanged—all before the case is brought to court. There might also be situations in which contributors with important information may not want to reveal their identity, so you'll want to guarantee the anonymity of specific external communication. Furthermore, the data stored and processed for the project should generally be secure. You realize that there'll be a need for a

shared working platform like a common server or a cloud solution to allow every employee access to the data needing protection. This applies not only to the data for investigating cases, but also to whoever does the accounting. Also, the social media accounts of the organization should be protected against hacking: A successful attack may not reveal sensitive information about cases and sources, but it would damage the reputation of the organization and the trust of sources in your professionalism. ■





## Question 2

### Who are our attackers?

*In a perfect and peaceful world, nobody would have to worry about digital assets like passwords or cloud data. But that's not the case. In this chapter, you will learn which attackers will likely target international development projects and to what extent.*

Your objects of protection (called “assets”) will only be at risk if someone targets them. Digital security is not a clear, achievable goal, but rather a shield of protection against some possible risks or attacks. That is why threat modeling looks at potential attackers and estimates the chance of successful attacks. This can be discouraging if the list becomes quite long, or motivating, if some assets are not at risk at all.

This section will introduce attackers that are common in international development. You will learn who they are, how and what they target, and how different attackers may be related. We use the word “attacker” broadly, for people and other challenges that put your assets at risk. For example, employees can be attackers if they are unaware of risks they pose, are not very knowledgeable about digital technology or don't understand the limitations of IT systems. Before we show you how to identify your attackers, we will explore concepts and types of attackers.

#### External attackers

Governments, social media platforms, criminal hackers, online trolls... The list of people who might target your data

can be never-ending. But with some structure, it is not that hard to evaluate. We can simplify the task by grouping attackers into three categories, based on their motivations and abilities to target you: state-related, commercial or personally-motivated attackers. The key questions to ask are: Who are they? Why would they target you? And how can they try to get your data?

#### State-related attackers

**Who?** A state is a complex entity with many different authorities that collect information for many purposes. For example, the police collect data predominantly to investigate crimes, while the goal of intelligence agencies is “simply” to gather information about trends in society to predict potential threats in advance. In theory, the exchange of information between state agencies or bodies should be governed and limited by laws. However, the limitations of powers cannot be guaranteed; even in democratic societies there are plenty of legal ways for authorities to share their information with one another. That's why we generalize and list “the state” as a potential attacker.

**Why?** Authorities, especially of governments receiving aid through international development you are working in, are by definition interested in your project activities. The aim of international development is to create positive social change, i.e. to strengthen democracy, protect human rights of marginalized groups or support building public infrastructure—and even if the government supports that aim, it is interested in just how far your influence and project reach.

**How?** As the state has a monopoly on power, it is often your most powerful attacker. Several authorities have technical capabilities to intercept communication or hack devices, legal rights to physically get information, maybe by searching property, and the right to access data collected by companies.

#### Commercial attackers

**Who?** With this category, we don't just mean every company. This refers to companies that process data of their customers. That applies to both companies that offer their products on and offline. The bottom line is that many of the services you use today require data about you. Relevant companies you should consider are: internet and telecommunication service providers, VPN providers, email service providers, social media companies and search engines, communication services like chat apps, voice and video call apps and cloud services to store data online, online advertising networks, transportation companies (like railway companies and airlines), banks and other external service providers that you use.

**Why?** Given financial gain is the purpose of a company, data collection and monitoring of its customers is done for profit. They collect data to either make sure that their service works properly (e.g. so users can log in, they store usernames and passwords), or to track users' online behavior on their platform (e.g. to improve the usability of the service, to show personalized advertisements or to sell data).

**How?** Basically, there are two ways for the entity to get your data: Either you provide it actively (e.g. when you register with your name or give bank details for the payment) or your online behavior is passively tracked (e.g. when you use social networks, browse the internet or use an email service).

### Personally-motivated attackers

**Who?** There are various individuals or groups of individuals that could be interested in the assets you are protecting. Think of corrupt colleagues, former bosses, ex-partners, and financially-motivated hackers, trolls on social media, supporters of the government, influential business people, companies you criticize publicly, or even terror organizations. What they have in common is that they have no legal way to obtain your data, other than the state (for the purpose of governance and control) or companies (for the purpose of financial benefit). Instead, they have to literally steal it illegally.

**Why?** Their motivations will be unique. Criminals are mostly interested in your assets because they can make money off them; attackers like trolls, government supporters or terror

organizations have political or ideological motives; personal attackers like ex-partners or colleagues may have a personal reason for their actions.

**How?** In general, personally-motivated attackers have less sophisticated tools at their disposal than commercial and state-related attackers. That is because they do not have the resources of large companies or states and also do not have the means to coerce you. However, this does not mean that they are ineffective in meeting their goals: If an online troll only wants to target you on social media, a Facebook account will be enough; if a hacker collective wants to get your bank details, a sophisticated phishing attack against your administration employees will be sufficient; if a terror organization wants to kill you, knowing the code to your office door can be enough.

### How external attackers are connected

We categorize attackers based on a set of motives or abilities that they tend to have, but they don't act in isolation. Actually, they are often connected which increases the risk posed to your data. During threat modeling, you will consider how an attacker can get access to your assets, but it is important to think of how an attacker might obtain your data indirectly. Diagram 4 shows the basic connections between groups of attackers.

A basic, but discouraging rule applies: If data exists, it will be used—but you cannot certainly know by whom. It is also not clear what workflows put your data at risk. If a telecommu-

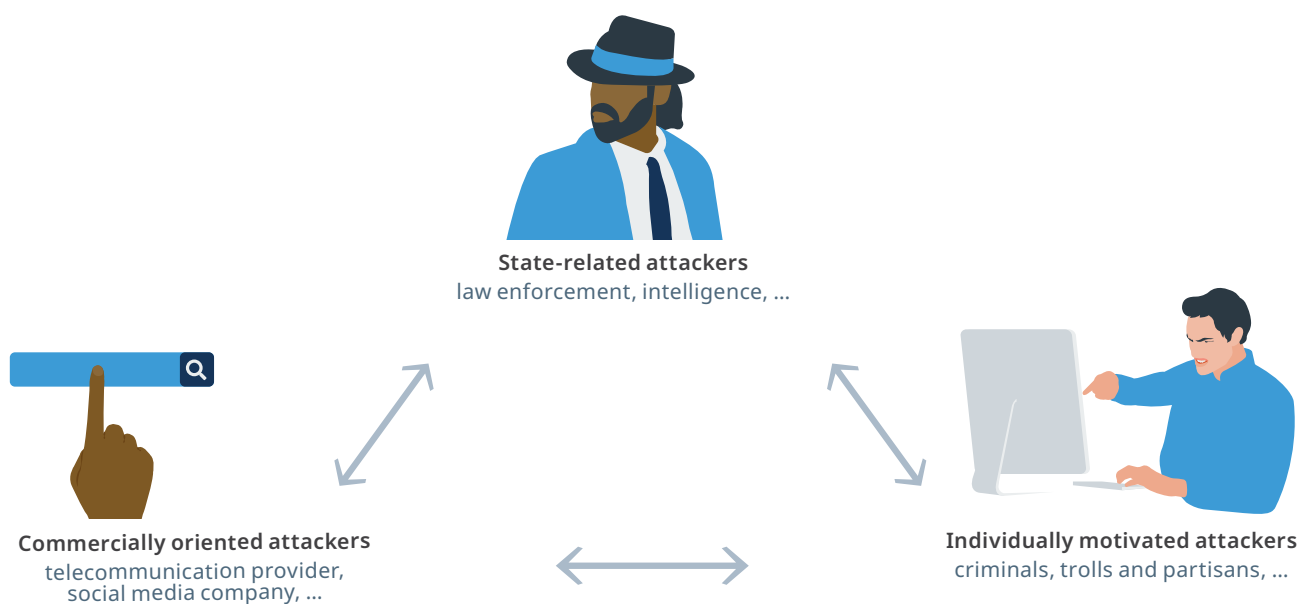


Diagram 4 Three groups of attackers

nication provider were to analyze your system data, it would not pose a large risk, however access to such data by the state may be of serious concern to you. Threat modeling will help you understand how much protection data needs in certain circumstances.

## How data is exchanged amongst different entities

The state's monopoly on power means they can put pressure on nearly anyone to provide certain information, for example overtly in an investigation, or secretly via surveillance. This dynamic is especially relevant to the relationship between the state and companies. Social media platforms collect data about their users primarily to make money, by profiling users based on their interests so they can target them with personalized advertisements. State authorities, however, can legally force the social media platform to hand over login data, chat protocols and usage data to learn more about suspects. As a result, commercial data ends up in the hands of the state and could be used against a user in a criminal investigation. This might have a positive impact, for example, if the police are able to gather further evidence against criminals, like drug dealers or murderers. However, if your project's activities were to be criminalized and investigated, and your data could be legally accessed, this would mean your project and partners (secret sources) are at risk.

The relation between state-related and personally-motivated attackers is less structured and often situational. Politically motivated online trolls may incite a campaign against your organization and try to take over your social media accounts — even if the trolls have no direct connection to the politicians they want to support. They just “want to do something” to support the government. If we flip this dynamic, it could be an internal connection, such as your former boss who is loyal to you, but is approached by an intelligence agency and forced to talk about things that the two of you actually want to hide from the government.

The same is often true for the relation between individuals and companies: They are loosely related and depend on the situation. You wouldn't think the two have any connection, but influential individuals might have strong relations to a big corporation, for whatever reason. However, these connections are mostly obvious: If it is well known that a terrorist group often receives money from a company, you should consider both as attackers.

## Step 4: Identify your potential attackers



After listing the assets you want to protect, make a second list of your potential attackers. You can pick them from a “pool” of attackers. Some of them are general, others might be specific for your particular project. Potential attackers in international development projects can typically be divided into three groups: state-related, commercial and personally-motivated attackers.

### How it's done



Every asset you want to protect has to be matched with its potential attackers. To identify these, refer to the information we provide in this guide. Consider the broader context of your project with the help of your team and conduct further research.

### Exercise 4: Think-pair-share to identify attackers



Gain insight and share knowledge using the “Think-Pair-Share” method we used in the workflow assessment in exercise 2. The idea is simple: First everybody thinks about a question on their own. Secondly, everybody exchanges their thoughts with a partner, and finally, everything is presented to the group.

As a project manager, use this method with your team to compile a list of all attackers. First, everybody takes five minutes to write down attackers on their own. Then in pairs, everyone spends five minutes sharing their results. Lastly, use 15 minutes to collect all results in a group discussion. During the group discussion, add each attacker to a table so everyone can see the full list. ■

### Exercise 5: Research typical attackers in the implementation country




Local insight is helpful in identifying attackers, so we suggest going beyond this brainstorming exercise (4) and conducting some research. You might hire local consultants and/or experts for a short analysis of the entire “threat situation” in the country your project is being implemented in. You'll find a list of guiding questions and research questions in the annex. ■

Using the table you created in exercise 1, you will now link each asset to all of the attackers. Doing this creates a path for each possible combination of asset and attacker. You can do this in a new column to the right of the existing table. Keep

in mind you'll need more space for the following steps and either use a large piece of paper or do it digitally. Moving forward, you will fill out each path as a separate risk scenario.

**Case study:  
Protection from the government—and others**

 Due to the kind of asset you want to protect, you realize the national government where your project is being implemented poses the greatest threat as an attacker. You want to bring cases where the fundamental right to freedom of expression was violated to court. Freedom of expression was most likely violated by state authorities or highly-influential politicians.

In analyzing the country's legal system, you soon realize that there are two groups of commercial attackers. Firstly, the national telecommunication and internet service providers are fully regulated by the state. The companies have to provide access to calls and internet connections and also

obtain metadata, like who called whom yesterday in your partner organization's city. Secondly, the national parliament recently passed a law in which "online companies" like social networks, email providers and cloud services available in the country, are legally bound to provide data upon government request. However, it is not yet clear whether the foreign-based internet companies will comply.

You identify two potential, personally-motivated attackers: trolls on social media, who either try to hack your online accounts or start hate campaigns against your organization and staff members; criminal hackers, who want to steal your bank credentials and make money.

Lastly, the data protection authority of the funding country in Europe is an attacker. As the project is financed with EU funds and your organization processes data within the EU, the European data protection law applies to your project. The data protection authority might impose high financial penalties if you do not comply.



Diagram 5 Example of an attack on an object of protection

## The human factor and internal resistances

There's a saying among IT specialists: "The problem is in the chair, not in the computer." The following example illustrates the "human factor".

### Example: WannaCry



In May 2017, the so-called "WannaCry" virus infected more than 200,000 computers across 150 countries. The ransomware encrypted all files on the infected devices and made them inaccessible.

This dramatic case shows how crucial the "human factor" in digital security is: "WannaCry" used a vulnerability in the software an older version of windows, but it was patched by Windows soon after its discovery—and two months before the "WannaCry" attack took place. If everybody had followed the recommendation to install the patch, the wide-reaching attack would not have been possible at all. ■

Technology is always used by humans, and humans make mistakes. That is why human behaviors have to be considered in threat modeling. You can have the most secure technology available—but it is worthless if employees do not use it properly because they were never trained, it is too complicated or they do not understand the possible threats it poses. We conducted interviews with international development project managers and consulted with experts. The most frequently mentioned kinds of compromising human factors and internal resistances are listed below. These can be divided into three overall groups: knowledge-based factors, structural barriers and organizational deficiencies.

### Knowledge-based factors



**Lack of knowledge:** Staff at every level of the organization simply do not know (enough) about digital security and the online risks in their work. They haven't been told that a regular email is comparable to a postcard that can be read by many entities during the transmission process.

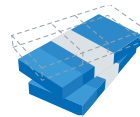


**Lack of awareness:** People at every level of the organization know that certain practices are not secure, but they resist implementing countermeasures because they are not aware of potential risks. For example, they know that a regular email is not secure, but they underestimate the chances of it being intercepted or think they "have nothing to hide".



**Lack of role models:** It is common that people in higher levels of an organization lack knowledge and awareness of IT security, including project managers or even CEOs. That is a problem not just for the "operational part" of the organization. This is both discouraging for staff trying to improve digital security in the organization and does not motivate others who need training to seek it.

### Structural barriers



**Lack of financial resources:** The organization may have not enough money to buy secure devices software, including updating to the latest versions. Also hiring specialized staff, like IT security experts, external consultants and tech trainers costs money.



**Lack of time:** Digital security is often considered "nice to have" and put off indefinitely for "when we have time." Digital security practices are, by definition, preventative, meaning the threats are not visible in everyday life. This makes it hard to conceptualize and easier to prioritize other pressing issues in a project.



**Impractical solutions:** Even if the organization's solutions are secure in theory, they may not be feasible when put into practice in your project. Maybe your organization has email encryption software, but it is too complicated and not required, so only a few people can be reached on it. Staff may not be motivated to use it and the security measures may have loopholes, meaning the encryption has little to no impact. This commonly happens when there is a gap between those "working on the ground" and the IT department responsible for infrastructure. Something might be simple for your IT team to implement or be a solution they think is user friendly, but not if your users are not tech natives.

### Organizational deficiencies



**Lack of rules and guidance:** The IT infrastructure is often not controlled by the IT department. This means people will use the easiest solution, like private devices for project-related tasks or unapproved software that is considered to be insecure, but practical. Sometimes this happens because IT is unaware, there are structural barriers, or employees don't understand why

software needs to be approved by a system administrator. Commonly these cases arise due to a lack of policy or rules to regulate workflows and devices.



**Lack of responsibilities:** Some organizations may have rules, but no one is responsible for enforcing them, so adherence is not monitored and noncompliance goes without reprimand. It is important that the need for a digital security concept is

acknowledged and supported at the management level which includes a willingness by so-called C-levels (like CEOs, CSOs, etc.) to improve their tech know-how.

### Step 5: Identify your digital security concept's internal challenges



You should also take human factors and internal resistance into account as “attackers”, and add them to your attacker list. Use the three overall groups, namely knowledge-based factors (lack of knowledge, lack of awareness, lack of role models), structural barriers (lack of financial resources, lack of time, impractical solutions) and organizational deficiencies (lack of rules and guidance, lack of responsibilities) to clearly list these.

#### How it's done



The human factors do not have to be matched with assets, because they are a threat to all assets. That means if you have structural deficiencies in your organization, most of them will apply to all your security mechanisms. Two examples:

**Lack of rules:** If there's no rule that prevents employees from installing unauthorized software, they might install unapproved software on devices. This one missing guideline impacts many workflows.

**Lack of knowledge:** If employees lack a general understanding of technology and digital security, a single tool or protection measure may do little to help the organization. Several loopholes in the security concept would remain.

#### Case study: Lack of...everything?



After looking at the project timeline, your budget and talking to the staff members at your local partner NGO, it is clear that enforcing a digital security concept will be a huge challenge. The organization does not have a uniform IT infrastructure, but follows the “bring your own device” concept: everybody uses his or her own private devices for professional purposes, and there is very little knowledge about digital risks. Due to the long-ruling autocratic government, the staff is also not aware of the dangers they face online, but rather accept threats cynically. The biggest concern is a loss of money from hacking attacks. There are plenty of stories about similar cases in other organizations in the country. There are no rules in place for IT security.

You are skeptical of whether your own organization is well prepared. You have had discouraging experiences with the IT department: you feel like they don't support you, but rather offer impractical solutions like proprietary software that no one else out there uses, or they just say: “This is not possible.” In the project plan, there is also no budget for digital security training, new devices or secure software solutions. And there is no realistic time planned to

Object of protection	Known mistake	Human factor
Internal communication via Skype	“I don't know whether Skype is secure.”	Lack of knowledge
Login credentials for social media accounts	“We use the same password for everything, even though the password guidelines forbid that.”	Lack of responsibilities
Research on the internet	“I would like to use Tor to be anonymous, but I do not have the admin rights on my computer to install the software.”	Impractical solutions

Table 3 Human factors as digital security threats

address security. You feel it is your responsibility, as a project manager, that the project staff is able to “take appropriate actions to work with sensitive data and therefore ensure the professional standards of the organization”. Unfortunately, you cannot find resources on this within the intranet, but there is a data commissioner in the organization that you can contact. ■

As these human factors apply to the entire threat model, they will be on a separate list at the end of the threat model, right after the long table. These “human factors” are somehow cross-cutting and therefore apply to all measures you will take: If the staff has little knowledge about IT, it has to be trained holistically. If the organization has no internal rules, those have to be created and implemented—for all assets and threats. To identify these “internal vulnerabilities”, we suggest your team do exercise number six.

### Exercise 6: The real reason



People often know that they could do things better, but certain environmental restrictions mean they don't and they keep working in an unsecure way. What's the real reason? To answer that, you have to identify the “human factor” in your security assessment by listing and then asking about the real reason.

For your list to be complete, start with your assets to protect. (If you are working in a group, divide into smaller groups or have everyone work on their own.) List all “known mistakes”—they prevent you from protecting the assets you actually want to protect. In a group discussion, ask what the real reason is. Maybe someone does not use a secure phone because your IT department does not allow you to install apps on the organization's phone. This would be a structural barrier. It might help to introduce the list of potential human factors before the exercise from above. This guides people and saves time, as you don't start thinking about the topic from the beginning. ■

Make a list of human factors that apply to all assets in the threat model. This will be helpful for anyone involved in setting up a security concept for your project. For example, if they know that there's a lack of knowledge, they may suggest doing regular training. If guidelines are missing, they can support in setting them up.





**Question 3**

**Are our attackers able to succeed?**

*So far, we mostly made assessments about both assets and potential attackers. Now, the real “modeling” begins and you will match assets with attackers so you can guess if they can succeed. If so, you definitely should protect yourself against them.*

After you identify both your assets and your potential attackers, the first part of the threat modeling process is done: the analysis of your professional environment and needs. This provides a solid foundation for the next phase: You can now estimate the likelihood and consequences of attacks.

This part is more hypothetical than the first one, but very crucial since you will not have enough time and resources to protect your project against all potential threats. Questions three and four help you to prioritize your tasks for your individual security concept. The result is a list of threat scenarios to close the biggest loopholes in your digital security concept.

To know if your attackers pose a risk to your assets, you have to match them. Only look at the external attackers, like state-related entities, not the human factors and internal resistances (see previous chapter).

Consider every asset and ask yourself whether your attackers are able to succeed with an attack, and if so, why (or why not?). For example, you want to protect the confidentiality of your communication via regular phone calls. If there aren't any attackers who would have interest or abilities to target it, then the asset isn't realistically at stake. Should the local government be an attacker with both the technical capabilities to intercept it and the legal right to get access from the national telecommunication service providers, you cannot ignore it, but need to continue the threat modeling for that specific path. At this stage, you should start to inform yourself more about the capabilities of your attackers. In the next steps, we'll provide some tips about where to find information and contact partners.

Object of protection	Attacker	Able to succeed?	Why (not)?
Object of protection 1	Attacker 1	✓	● Legal and technical capabilities
	Attacker 2	✓	● Technical capabilities
	Attacker 3	X	● No interest
Object of protection 2	Attacker 1	X	● No capabilities
	Attacker 2	X	● No interest
	Attacker 3	X	● No interest, but technical capabilities

Table 4 Matching objects of protection and attackers | high risk ● moderate risk ● low risk ●



### Step 6: Matching your assets with attackers



Now that the assets to protect are matched with all potential attackers, you will shorten the list. This process will make real risks clear and focus your efforts.

#### How it's done



Enter all assets in the first column with as much detail as possible. In the second column, record potential attackers to each single asset. For inexperienced project managers, it is enough to only distinguish between the three broad attacker groups, namely state-related, commercial and personally motivated. In the third column, answer the guiding question, "Is the attacker able to succeed?" A short explanation in the fourth column helps to qualify the decision and will be used as a starting point for the next step. From here on, we will focus on prioritizing threat scenarios.

This table will help structure your threat model. As you can see, this step is especially helpful to reduce the number of relevant threats. Considering the amount of objects to protect combined with a long list of potential attackers, you may feel lost and discouraged. By breaking it down and realistically analyzing what your attackers are interested in, however, you will see that some of your perceived dangers actually don't exist.

For the first column, you should be as detailed as possible. List all the assets, particularly your workflows, and create a path for each one. This means you will have one path to cover each possible combination of factors.

For the attacker column, being detailed is also important. Refer to research you did in **question 2**, especially with external resources, if you need help estimating their chances of success. Also, individual research on the situation in the country and its legal system is crucial, as well as discussions with partner NGOs in the country.

### Case study: The potential of your attackers

Collect all your assets and match each of them with all potential attackers.

#### Communication within the team and with external partners

Object of protection	Attacker <sup>1</sup>	Likelihood <sup>2</sup>
Shared information  Calls via landline Example: Current project status (2), research strategies (3), sources for research (3), budget information (1), administrative information (1), travel planning (1), ...	National government	● Strong interest, technical capabilities to intercept communication and legal rights to obtain data from companies
	National telecommunication and internet service providers	● Little commercial interest, but technical capabilities to intercept communication routed via their infrastructure and legal obligation to grant access to national government
	Social networks, email providers and cloud services	● No access to infrastructure, no commercial interest
	Criminal hackers/trolls on social media	● Interest, but no access to infrastructure
	Data protection authority in the funding country	● Probably low interest, and only access for communication within the funding country; probably no legal right to intercept communication on the basis of data protection law

**Table 5** How to match assets and attackers – an example | <sup>1</sup> To reduce the number of columns, attackers with the the same ability to succeed are listed together. | <sup>2</sup> Please note that this is just an example to demonstrate how a threat model can be done. The capabilities of attackers differ from country to country, and digital technology is evolving. | high risk ● moderate risk ● low risk ●

Continuation of table 5

**Communication within the team and with external partners**

Object of protection Shared information	Attacker	Likelihood
<p><b>Calls via Skype</b> Example: Project status updates (2), research strategies (3), sources for research (3), budget information (1), administrative information (1), travel planning (1), ...</p>	<p>National government</p> <p>Skype</p> <p>National telecommunication and internet service providers / social networks, email providers and cloud services</p> <p>Criminal hackers / trolls on social media</p> <p>Data protection authority in the funding country</p>	<p>● Strong interest, but maybe no technical capabilities to intercept communication, and maybe no legal agreement with Skype</p> <p>● Little commercial interest, but technical capabilities to intercept communication routed over their infrastructure and maybe legal obligation to grant access to national government</p> <p>● No access to infrastructure, no commercial interest</p> <p>● Strong interest, but only low sophisticated capabilities (e.g. phishing of Skype account information), and no legal measures to get data</p> <p>● Probably low interest, and probably no technical access to intercept communication, and probably no legal obligation to intercept communication the basis of data protection law</p>
<p><b>Emails over own email server, often sent to third-party email providers like Gmail, Yahoo (encrypted in transit)</b> Example: Project status updates (2), research strategies (3), sources for research (3), budget information (1), administrative information (1), travel planning (1), ...</p>	<p>National government</p> <p>Third-party email providers</p> <p>National telecommunication and internet service providers / social networks and cloud services</p> <p>Criminal hackers / trolls on social media</p> <p>Data protection authority in the funding country</p>	<p>● Strong interest, but maybe no technical capabilities to intercept communication, and maybe no legal agreement with third-party email providers</p> <p>● Little commercial interest, but technical capabilities to intercept communication routed over their infrastructure and maybe legal obligation to grant access to national government</p> <p>● No access to the infrastructure, no commercial interest</p> <p>● Strong interest, but only low sophisticated capabilities, mainly phishing via email to get passwords, and no legal measures to get data</p> <p>● Probably low interest, and probably no technical access to intercept communication, and probably no legal obligation to intercept communication on the basis of data protection law</p>

Object of protection Shared information	Attacker	Likelihood
<p><b>Chats and calls via instant messaging apps like WhatsApp, Signal (end-to-end encrypted)</b>                      Example: Current project statuses (2), research strategies (3), sources for research (3), budget information (1), administrative information (1), travel planning (1), ...</p>	National government	<ul style="list-style-type: none"> <li>● Strong interest, but probably no technical capabilities to hack into end-to-end encryption</li> </ul>
	End-to-end encrypted messengers like WhatsApp, Signal	<ul style="list-style-type: none"> <li>● Neither interest in content, nor technical capability to see the contents due to end-to-end encryption (metadata may be accessible)</li> </ul>
	National telecommunication and internet service providers / social networks, email providers and cloud services	<ul style="list-style-type: none"> <li>● No access to infrastructure, no commercial interest</li> </ul>
	Criminal hackers / trolls on social media	<ul style="list-style-type: none"> <li>● Strong interest, but most probably no technical capabilities to hack the end-to-end encryption</li> </ul>
	Data protection authority in the funding country	<ul style="list-style-type: none"> <li>● Probably low interest, and probably no technical access to hack the end-to-end encryption</li> </ul>

**Anonymity of external communication (metadata)**

Object of protection Shared information	Attacker	Likelihood
<p><b>Phone calls via landline</b>                      Example: Identity of sources and/or undercover employees including data that reveal their identity, e.g. phone number (3)</p>	National government	<ul style="list-style-type: none"> <li>● Strong interest, technical capabilities to intercept communication and legal rights to obtain data from companies</li> </ul>
	National telecommunication and internet service providers	<ul style="list-style-type: none"> <li>● Little commercial interest, but legal obligation to obtain data to the government</li> </ul>
	Social networks, email providers, cloud services, etc.	<ul style="list-style-type: none"> <li>● No access to the infrastructure, no commercial interest</li> </ul>
	Trolls on social media / criminal hackers	<ul style="list-style-type: none"> <li>● Some interest, but neither technical nor legal capabilities to get data</li> </ul>
	Data protection authority in the funding country	<ul style="list-style-type: none"> <li>● No interest, no access to infrastructure, no legal rights to obtain data from telecommunication companies,</li> </ul>

Continuation of table 5

**Anonymity of external communication (metadata)**

Object of protection Shared information	Attacker	Likelihood
<p><b>Internet based calls (VoIP), e.g. over Skype, WhatsApp, Signal (encrypted in transit and/or end-to-end)</b> Example: Identity of sources and/or undercover employees including data that reveal their identity, e.g. phone number (3)</p>	<p>National government</p> <p>National telecommunication and internet service providers</p> <p>VoIP services like Skype, WhatsApp, Signal</p> <p>Trolls on social media/criminal hackers</p> <p>Data protection authority in the funding country</p>	<p>● Strong interest, but probably no technical capabilities to hack into encryption, maybe legal agreement with services</p> <p>● No interest, no access to data</p> <p>● Access to data, maybe commercial interest to store data, and maybe legal agreement with governments to obtain data</p> <p>● Strong interested, but most probably no technical capabilities to hack the encryption</p> <p>● Probably low interest, and probably no technical access to hack the encryption</p>
<p><b>Emails via own email server, often sent to third-party email providers like Gmail, Yahoo (encrypted in transit or end-to-end)</b> Example: Identity of sources and/or undercover employees including data that reveal their identity, e.g. phone number (3)</p>	<p>National government</p> <p>National telecommunication and internet service providers</p> <p>Third-party email providers</p> <p>VoIP and messaging services like Skype, WhatsApp, Signal</p> <p>Trolls on social media/criminal hackers</p> <p>Data protection authority in the funding country</p>	<p>● Strong interest, but maybe no technical capabilities to intercept communication, but maybe legal agreement with third-party email providers</p> <p>● No access to the infrastructure, no commercial interest (only access if emails are not encrypted in transit)</p> <p>● Little commercial interest, but technical capabilities to intercept communication routed over their infrastructure and maybe legal obligation to grant access to national government</p> <p>● No access to the infrastructure, no commercial interest</p> <p>● Strong interest, but only low sophisticated capabilities, mainly phishing via email to get passwords, and no legal measures to get data</p> <p>● Probably low interest, and probably no technical access to intercept communication, and probably no legal obligation to intercept communication on the basis of data protection law</p>

Stored and processed data

Object of protection Shared information	Attacker	Likelihood
<p><b>Stored and processed data on the organization's own server</b> Example: Nearly all information that are processed in the project (1-3), including research (3), staff information (1), banking information (2)</p>	<p>National government</p> <p>National telecommunication and internet service providers / social networks, email providers and cloud services, etc.</p> <p>Trolls on social media / criminal hackers</p> <p>Data protection authority in the funding country</p>	<ul style="list-style-type: none"> <li>● Strong interest, but probably no hack the server, maybe legal rights to search the server</li> <li>● No access to the server</li> <li>● Strong interest, but probably no technical capabilities to hack server remotely</li> <li>● Maybe some interest, but probably no technical capabilities to hack the server or search it</li> </ul>
<p><b>Stored and processed data on a third-party cloud service</b> Example: Nearly all information that are processed in the project (1-3), including research (3), staff information (1), banking information (2)</p>	<p>National government</p> <p>Used cloud service</p> <p>National telecommunication and internet service providers, social networks, email service providers, etc.</p> <p>Trolls on social media / criminal hackers</p> <p>Data protection authority in the funding country</p>	<ul style="list-style-type: none"> <li>● Strong interest, but probably no technical capabilities to hack the cloud, maybe capability to get login data through phishing, maybe legal agreement with cloud service</li> <li>● Little commercial interest, but to get data stored in the cloud, and maybe legal obligation to grant access to national government</li> <li>● No access to the cloud</li> <li>● Strong interest, and maybe capabilities to get login data through phishing</li> <li>● Maybe some interest, but probably no technical capabilities to hack the server, maybe legal agreement with cloud provider</li> </ul>

Continuation of table 5

**Accounting and bank details**

Object of protection Shared information	Attacker	Likelihood
<b>Accounting and bank details stored on the system of a bank</b> Example: Bank records and transactions (2), Log in data for bank account (3)	National government	● Maybe interest, and maybe legal agreement with the bank
	Bank	● Access to all data, no interest to share data, but maybe legal obligation
	National telecommunication and internet service providers/ social networks, email providers and cloud services	● No access to data
	Trolls on social media	● Little interest, and probably no technical capabilities to circumvent security measures of the bank system
	Criminal hackers	● Strong interest, and probably technical capabilities to circumvent security system of the bank
	Data protection authority in the funding country	● Some interest, and maybe legal agreement with bank

**Online account credentials**

Object of protection Shared information	Attacker	Likelihood
<b>Social media accounts</b> Example: Username and password for accounts that are not protected with two-step authentication (3)	National government	● Strong interest, maybe technical capabilities to get login data through phishing, maybe legal agreement with social networks
	National telecommunication and internet service providers/ email providers and cloud services	● No access to the infrastructure
	Used social networks	● Access to the data, no commercial interest to share them, but maybe legal obligation to obtain them to governments
	Trolls on social media	● Strong interest and potential to hack weakly protected accounts through social engineering (phishing etc.)
	Criminal hackers	● Little interest, but probably technical capabilities to get data through phishing
	Data protection authority in the funding country	● Little interest and probably neither technical nor legal measures to get the data

## Case study results

All your assets are of interest or relate to at least one of your attackers. You will have to continue threat modeling for each of your assets, but you can leave out some of your attackers. These assets are at stake against the attackers in the following scenarios:

- **Communication within the team and with external project partners:** the strongest attacker is the national government that has technical capabilities to intercept communication and also certain lawful ways to obtain communication data, especially from companies based in that country; companies do not have a commercial interest in your communication, but may be legally bound to provide it to the state; criminal hackers may have capabilities to hack certain communications, but are only interested in it if they can make money out of it. Using services that have end-to-end encryption is very important!
- **Anonymity of specific external communication (e.g. sources, undercover employees):** the strongest attacker is the national government that has technical capabilities to intercept communication and also certain lawful abilities to obtain communication data, especially if the company is based in the country; companies do not have a commercial interest in your communication, but may be legally bound to provide it to the state; criminal hackers may have capabilities to hack certain communications, but only have interest in it if they can make money out of it.
- **Stored and processed data (on the organization's server or on a cloud):** the strongest attacker is the national government that has technical capabilities to hack your server or your cloud, and also legal rights to obtain stored data from server and cloud providers, especially if they are based in the country; companies have access to data stored on their infrastructure, but no commercial interest to use it against you; criminal hackers have a strong interest in your stored data to get bank details, and therefore may develop sophisticated hacking and phishing attacks; the data protection authority of the funding country can legally force you to provide certain data.
- **Accounting and bank details:** the strongest attackers are criminal hackers who want to make money out of your accounting and bank details and therefore develop sophisticated hacking and phishing attacks; the data protection authority of the funding country can legally force you to obtain certain data; the government has only a little interest in that kind of data, which is why an attack unlikely—but if they wanted to, they could use technical or legal measures to get it; companies only have access to it if it is stored on their infrastructure, but no commercial interest to use it against you.
- **Social media accounts:** a lot of your attackers are interested in your social media accounts, especially the government, which has both technical measures to hack the accounts and certain legal rights to get data from the social media companies; trolls on social media have a strong interest and can develop moderate attacks to hack accounts with weak protection; the social media companies have access to your accounts, but no commercial interest to use it against you; criminal hackers only have interest in bank details, so they develop sophisticated phishing and hacking attacks to get access to your social media accounts.



## Question 4

### How likely is it that your attackers can successfully attack you?

*Every project has many vulnerabilities and potential threats, and no one has enough resources to prevent all of them. In this chapter we will learn how to prioritize threats in order to know where countermeasures are most needed.*

In the last part of the threat modeling process, you will assess likelihood. Once you are done, you will have identified specific scenarios where your assets would be at risk against particular attackers. The aim of this question is to set priorities to start with. If you have limited resources, you will know what you definitely have to spend them on.

Similar to the third question, here you will estimate how likely it is that certain things will happen and what factors could impact or decrease the likelihood. Working off the results of the attacker matching, you will bring these scenarios together with your workflows, your attackers' capabilities and consider the "human factors and internal resistances". Remember that the latter are not a single, but general threat which can increase the likelihood that an attacker is successful. You should not only do the likelihood estimation on your own, but also do some additional research and include others in the discussion, for example:



**Country reports:** Civil society organizations, business associations, supranational governmental organizations, like the UN, and others could have published reports about the country in the past and specifically about the digital rights situation.



**Local partner organization:** The local or national partner organizations have already faced violations of their rights, know what attacks are common in their country and can advise on the likelihood.



**IT department of your organization:** The IT department of your organization can support you with technical expertise and explain whether potential threats are possible or not. IT specialists are familiar with threat models.



**Data protection officer of your organization:** The data protection or internal compliance officer of your organization is well aware of both the legal obligations of your organization and past data breaches; their insight could help you understand the likelihood of attacks.



**International partner organizations:** There are several organizations that work on human rights and focus on digital security. They are important resources as they offer free consultancy, published guidance materials and reports with a digital rights focus.



**IT security companies:** Companies that provide the technology for your countermeasures are probably well aware of potential attacks and can explain whether their solutions may help you or not.



**Newsletters and social media:** Many news outlets cover digital security topics regularly. Stay informed and ahead of risks with a subscription to their newsletters, following their accounts and their technology journalists too, to catch posts on new developments, like new tools or vulnerabilities in existing software.



## Step 7: Estimate the likelihood of an attack



The last step of the threat modeling process gives you a practical outcome. You will apply the threat scenarios you identified within the context of your project. The result is a realistic assessment for each of the threat scenarios. This helps to find high, medium, low and non-existent threats in order to prioritize the need for specific countermeasures.

To be clear, finding and implementing countermeasures is not up to you alone, but your insights into the project will make this last step easier than you might think! You talk to experts about the likelihood of scenarios, do your own research and are in constant contact with your partner NGO in the country. They will certainly name some typical countermeasures. Take notes and include them at the end of the paths of your flow-chart or the last column of your table. Discuss your identified threat scenarios in detail with experts instead of focusing on broader information and assumptions.

### How it's done



You can add the likelihood to your table or flow chart. If you do it digitally, you should directly prioritize the threats, starting with the highest likelihood.

Potential countermeasures are not yet part of the threat modeling process. However, as you do research on your own and have conversations with experts, you should record everything you learn which will save you time and help you to remember advice. This does not have to be detailed, just recap their insights and how it applies to your project. For example, it might be enough to name 'encryption' as a countermeasure, while the concrete implementation with a particular encryption tool still has to be defined.

Threat scenario	Project context	Likelihood	Countermeasures
Threat scenario 1	Inherent to daily work, crucial workflow, high interest to an attacker and internal resistances within the project	High	Technical measures to protect the project infrastructure, training staff to use it
Threat scenario 2	Technically possible and human factors that can support an attack, but of no interest to attacker	Little	Raising awareness and training staff; clear guidelines for use of technology
Threat scenario 3	Theoretical interest to attackers, but neither technical nor legal access	None	None

Table 6 Possible factors to determine likelihood and potential countermeasures

### Case study: Guessing and estimating threats

Discuss every threat scenario you previously identified within the context of the project and potential, inherent challenges.<sup>1</sup>

#### External attackers

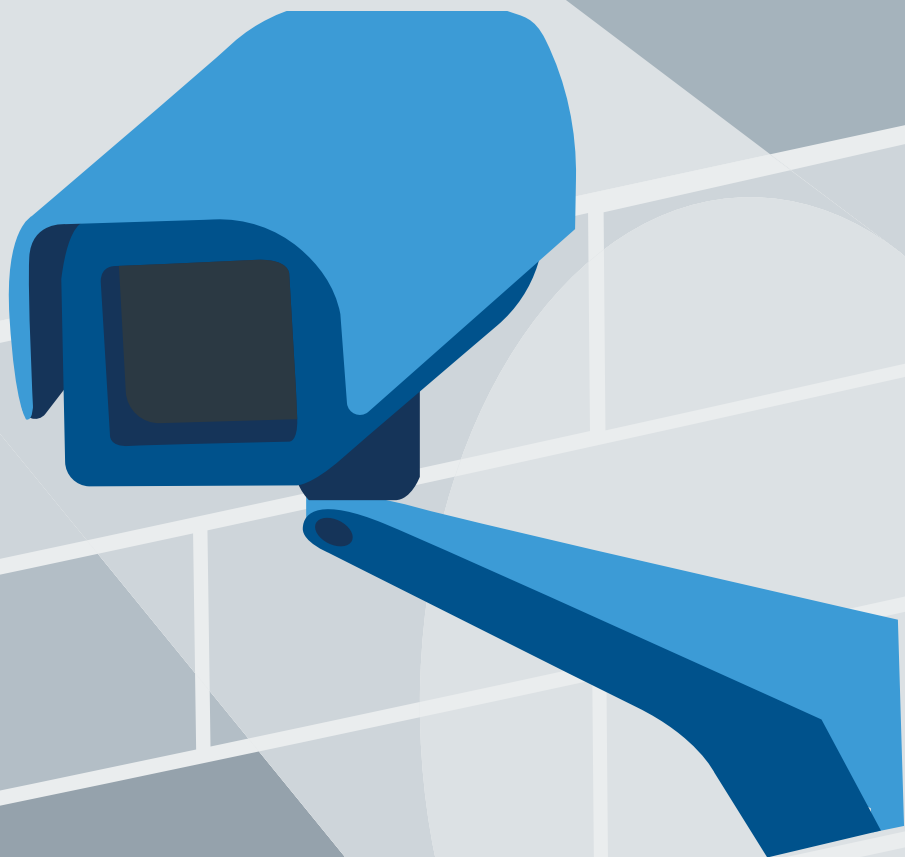
Threat scenario	Project context	Like- lihood	Countermeasures
National government of project country intercepts communication within the team or with external project partners	If voice-based communication (e.g. calls) is provided by the national telecommunication providers, they can grant access to the government	High	Use end-to-end encrypted calls over internet telephones, for example with chat apps; training for staff, since their familiarity with this technology is low
	If text-based communication (e.g. emails, chats) is provided by foreign, commercial service providers, they can grant access to the government	Medium	Make an analysis of the terms of service of the service provider and check whether they have a legal obligation to comply; use end-to-end encrypted services so that the company is technically unable to provide the content of the communication
	If the communication is end-to-end encrypted, the government can hack devices to circumvent the encryption	Low	Training of the staff to identify hacking attacks through phishing campaigns; internal technology guidelines to always have the latest updates installed in order to patch vulnerabilities; constant forensic analysis of the devices by IT experts; systematic protection by the organizations' IT department
	If the IT department provides a secure solution that does not meet the practical needs of the employees, they will use insecure communication channels	High	Make an evaluation of the practical needs and develop a communication strategy together with the IT department
Cyber criminals hack communication to obtain bank details	If the bank details are not protected well and the staff is not aware of typical attacks, like phishing, criminals might be successful	High	Reduce the number of employees that have access to the bank details, as well as training the staff, create a binding security guideline on how to use the bank account
Government uses legal means to get information from third party services like social networks, ISP, email service providers, etc.	If the company is based in the same country as the government, cooperation is very likely	High	If data is sensitive, these services should not be used
	If the company is not based in the country of the government, it depends on a legal agreement between governments and companies whether data can be obtained or not	Medium	Research if data can be lawfully obtained, and if so, avoid use of these services for sensitive data

### Human factors and internal resistances

Threat scenario	Project context	Likelihood	Countermeasures
Weakly protected, private devices open loopholes for viruses that infect the organization's infrastructure	As the organization allows its employees to use their private devices for business purposes, these devices may be weakly protected and not up to date in terms of security. If employees for example get a virus on their private computer, it may also affect the organization's server.	high	Use device management tools in order to be able to get access to the employees' devices, e.g. to force them to install the latest updates for software.

**Table 7** *Identifying threats and countermeasures based on the threat model | <sup>1</sup> This is a generic chart which is meant to demonstrate how certain threats can be summarized under threat scenarios, and give a few prevention tips.*

**Outcome: Towards your own  
digital security concept**



You have created a detailed and personalized threat model. And now...? In this chapter, we'll explain how to use a threat model to find a holistic security concept for your project.

A threat model is not yet a digital security concept, but the basis for one. It allows you to think of countermeasures for threats you prioritized. This could be done by project managers by themselves. With enough knowledge about the technical background of tools and experience using them, project managers are probably the best candidates to decide which tools may be used in their project — preferably it is discussed with the entire team.

However, the reality is different: Most of the time, project managers are not technical experts — and they do not have

to be. That is why we recommend consulting with experts who can develop a digital security concept. Refer to the list of potential contacts in **question 4** for ideas of who can help. They will likely know of tools which would help to prevent threats, and how to set up hardware and install software. If your organization has an IT department, they should know what tools are secure, fit your project's context, and can be implemented in your organization's infrastructure. If you do not have your own IT department, you can reach out to private consulting companies that address digital security, or reach out to other NGOs and ask them about their security concepts and experiences.

**Attack matrix, based on the previous case study**

<div style="display: flex; align-items: center;"> <div style="width: 10px; height: 100px; border-left: 1px solid black; margin-right: 5px;"></div> <div style="display: flex; flex-direction: column; align-items: center; justify-content: center;"> <div style="margin-bottom: 5px;">↑</div> <div style="margin-top: 5px;">↓</div> </div> </div>	<p><b>More capable and/or motivated attackers</b></p>	Autocratic government uses public reports to make up a politically motivated case, e.g. about "endangering national security" or "blasphemy"	Tax authority searches the office and confiscates computers to investigate supposed tax evasion	Criminals send sophisticated phishing links to staff members to get login data for online banking	Government technologically hack end-to-end encryption on team member's WhatsApp to identify sources
	<p><b>Less capable and/or motivated attackers</b></p>	Trolls use phishing to get login information for social media accounts in order to spread wrong information via the organization's account — and harm their reputation	Government intercepts regular phone calls of the organization due to a legal agreement with the national ISP	Government requests login data from a cloud service provider to get internal drafts for reports that will be published soon	An email service provider cooperates with a government due to a legal agreement and hands over highly confidential emails with sources that are not end-to-end encrypted
		Data protection authority finds errors in the privacy policy on the organization's website, issues fine	Criminal hackers target the organization with ransomware to encrypt all information on the server and get ransom for the decryption code	Religiously motivated activists break into the office and steal devices in order to find sensitive information about upcoming publications	Governments or political partisans send phishing emails to get access to the email inboxes of employees and get highly confidential communications
		Trolls use public reports to criticize staff members for their opinion, spark outrage and blackmail them	Trolls search the web and social media to get hints on employee travel e.g. due to GPS location of shared pictures	Political partisans try to hack into Skype accounts in order to see the communication history of employees	Motivated trolls search the internet for publicly available information in order to get hints for the identity of sources
		<b>Public information</b>	<b>Internal information</b>	<b>Confidential information</b>	<b>Highly confidential information</b>

Table 8 Example for a risk matrix based on a threat model

Start simply by developing an attack matrix to match the confidentiality of information with the capabilities of your attackers. This can give you an overview of your most important assets and attackers who could successfully attack them. As you have already evaluated the confidentiality of your shared information and estimated your attackers capabilities, you can use these assessments to create your matrix. Your matrix then serves as a tool and will clearly show what information is most at risk. This helps colleagues understand what kind of information is important to protect, and how they can be compromised.

Such a matrix can then also be a “call to action” since easy targets that are not well protected against attackers will be more obvious to you. Then it is important to find potential countermeasures.

Complete protection is not possible, of course, and it can be harder to protect yourself against a very skilled attacker, but these attacks are also less likely. So a pragmatic approach would be to go through the matrix, starting with the lower lines: First try to address relatively low-tech attacks by relatively low-motivated attackers. In our example, this means training your colleagues to not share too much information publicly so that trolls cannot easily blackmail them, and offer psychological help in extreme cases. Or set up rules for not sharing information that might put sources in danger.

This could be done line by line, preferably for all attacks that you find most relevant. To give you an idea of how those countermeasures might look, here is an overview with some basic but essential steps against common threats.

Threat	Potential countermeasures
Financially motivated criminals and social media trolls want to get login credentials for social media accounts	<ul style="list-style-type: none"> <li>- Regular training of staff to help them understand phishing, including new employees, interns, etc.</li> <li>- Binding requirement for two-factor authentication of organization's professional and private accounts, including their employees, and a process to enforce it (e.g. regular check by an internal security officer)</li> <li>- Anti-virus software on all devices used by employees to protect against ransomware and other malware on all devices</li> </ul>
Government intercepts communication	<ul style="list-style-type: none"> <li>- Regular training of staff in phishing, including new employees, interns, etc.</li> <li>- Binding requirement for two-factor authentication of organization's professional and private accounts, including their employees, and a process to enforce it (e.g. regular check by an internal security officer)</li> <li>- Anti-virus software on all devices used by employees to protect against ransomware and other malware on all devices</li> <li>- No use of landline or mobile phones for sensitive topics</li> <li>- As a default, use services with end-to-end encryption</li> <li>- Agreement with partner organizations about which communication services should be used</li> <li>- Information matrix to identify and explain what information needs the highest level of protection and why</li> </ul>
Data stored on computers and the organization's server are stolen in a burglary	<ul style="list-style-type: none"> <li>- Guidelines for offline behavior during calls, e.g. looking around for potential spies when sensitive issues are discussed</li> <li>- Binding office rules, dealing with topics such as locking doors, switching on burglar alarm systems, closing windows, etc.</li> <li>- Binding so-called OpSec rules (operational security), dealing with topics like “locking” devices with a password, having lockable cabinets, etc.</li> </ul>

Table 9 Examples for countermeasures based on a threat model

Unfortunately, it is hard to provide a “one size fits all” solution against threats. Every project is different with its own unique context and people—that is why a customized threat model will serve you best. There are, however, some situations that occur in most projects. Factor these common solutions into your own digital security concept. Some examples are:



Use open-source software! Open-source means that the code of a program is publicly available. Everybody can review it, search for vulnerabilities and develop it further. The opposite is “closed-source”, so that no one but the developer—e.g. a company developing an app—can review it. Especially if a service is popular, open-source is of real benefit. A lot of experts review the code and constantly improve it. Users do not have to believe what a service provider claims about their product or service—they can see how it works in the code.



Go for services with end-to-end encryption! End-to-end encryption means that even the service provider cannot access the content and only the sender and the recipient can read it. This is imperative for communication tools such as chat apps, voice calls or emails, end-to-end encryption used by human rights activists and their sources. Especially if the service is both end-to-end encrypted and open-source, it will be a real challenge for attackers to access data by hacking. But be careful: Some services offer end-to-end encryption, but only if a user switches it on. Many people do not know that and assume it is automatically turned on. Users need to be educated about services they use.



Three steps to protect accounts: strong passwords, anti-phishing training, two-factor authentication! The most important things you need to know about passwords are: A password should only be used for one service, and should be strong enough to survive a password cracking attempt. It is difficult to remember one or multiple strong passwords. It is recommended that you use a password manager that remembers your passwords for you, and protect it with a randomly generated passphrase. A password manager is a software tool that stores passwords for you. Your passwords will be encrypted and stored on your device in a password database. The encryption key is generated from one additional password or passphrase, that is not stored and that you have to remember. Employees should also be regularly trained to detect phishing through links or malicious attachments, e.g. through so-called phishing quizzes you can find online. Lastly, two-factor authentication (2FA) is essential today. The term two-factor authentication means that you need a second credential in addition to your password to log in to your account. This could be a code sent via SMS, a code created by a third-party app, or a security key that has to be plugged in to log in. 2FA is powerful, because even if an attacker gets your password, it cannot simply log in.



Update your software regularly! Software code is never perfect—and attackers are always looking for loopholes in a code to hack. That is why updates from the developers should be installed as soon as they are published—that applies to all software and devices used in the organization’s work. The organization needs to be able to enforce a security concept consistently for it to work; not knowing what hardware and software are being used by employees makes it hard to manage or advise on security.

Those rules and countermeasures are often addressed in policies. It is important that these policies are not too long and abstractly written, but are in “the language of employees”, including step-by-step explanations and images.

Furthermore, the policies can only be put into practice if the staff is frequently trained on them. This should be required for all new employees, new interns and other staff members who have not yet been trained. Lastly, a threat model and security concept have to be updated over time. Things change: new workflows are added, new needs to communicate arise or you may need to reestimate the threat a certain attacker poses, say after the election of an autocratic state leader. We recommend adjusting a threat model and security concept every three to twelve months (depending on what your resources and project realistically allow).

**Further reading: Information about digital security and data breaches**



NGOs: Access Now: “Digital Security Helpline”, Electronic Frontier Foundation: “Surveillance Self-Defense”, Reporters Without Borders: “Digital Security Helpdesk”, Center for International Media Assistance

Most of these media and organizations have regular newsletters you can subscribe to.

# Annex



## Group work: Threat modeling scenarios

### Walk through the park

---

You want to visit a friend who lives nearby, but you have to pass through a park without streetlights and some areas have no cellphone service. The way through the park, however, is the shortest one to your friend's house. But there are also other ways, for example a path alongside a big street with street lights and constant phone connection. This one is almost two kilometres longer, because you have to completely circumvent the park.

Please discuss in your group: In which scenarios would you choose the way through the park, and when would you prefer to take the pathway? While discussing, please make a list with arguments and specify:

- the assets you would like to protect while going to your friend's
- any potential attackers you think of and how they could attack,
- factors that influence the likelihood of an attack, and therefore your final decision.

Use eight minutes for your discussion. Please present your results in a short talk.

### Shopping

---

You want to buy new clothes for a party that will take place this evening. Although the city is very crowded today, you go out with a wallet full of cash. Usually, you put your wallet in a bag, but the zipper broke yesterday.

Please discuss in your group: In which scenarios would you still put the wallet in the bag, and when would you prefer other options—and what are they? While discussing, please make a list with arguments and specify:

- the assets you would like to protect while shopping,
- any potential attackers you think of and how they could attack,
- factors that influence the likelihood of an attack, and therefore your final decision.

Use eight minutes for your discussion. Please present your results in a short talk.

### Parking your car

---

You are on vacation and want to take a walk through isolated mountains with your friend. You stow your luggage in the trunk of the car, and you are now looking for a parking place. There is one in the valley, which is touristy, expensive and it is another seven kilometres away. However, it is patrolled by a guard. There is also another one, higher in the mountains, that is located perfectly for you, but not guarded.

Please discuss in your group: In which scenarios would you choose the touristy parking place and when would you choose the mountains? While discussing, please make a list with arguments and specify:

- the assets you would like to protect during your walk,
- any potential attackers you think of and how they could attack,
- factors that influence the likelihood of an attack, and therefore your final decision.

Use eight minutes for your discussion. Please present your results in a short talk.

### Customs control

---

You go to visit a close friend who lives on another continent. On the last day, you receive a local present worth \$2000. When you arrive home, you know that you have to pay a lot of taxes for it. At the airport you are free to choose whether or not you declare it at customs. What do you do?

Please discuss in your group: In which scenarios would you not declare and in which scenarios would you be honest? While discussing, please make a list with arguments and specify:

- the assets you would like to protect while traveling,
- any potential attackers you think of and how they could attack,
- factors that influence the likelihood of an attack, and therefore your final decision.

Use eight minutes for your discussion. Please present your results in a short talk.

## Table for your workflows

### Guiding questions

- Which workflows exist in the project?
- Which employees are involved in the workflows and how?
- Which information do you work with and share in the project?
- What services and software do you use? What hardware is needed?
- With whom do you communicate regularly?
- Think of all team members: What do you do with them?
- Think of yesterday: What did your day look like?
- Check your calendar: What does your regular week look like?
- Which devices do you use for job-related purposes? What for?
- Which software is installed on your computer? How does it relate to your workflows?

Workflow	Involved employees	Shared information	Used hardware and software	Object of protection

## Questions for your country research

### Guiding research questions

- Which entities — government, private, individual — are known to be the most critical of civil society in the country?
- Which laws allow these entities to interfere with the fundamental rights of members of civil society, e.g. through surveillance or detention?

### Detailed research questions

- What is the general structure of the security agencies, like law enforcement vs. ministries vs. intelligence agencies etc.? How do they depend on each other or how are they separate from each other? Is there a division of power?
- Which authorities are allowed to exercise surveillance in the country on a legal basis?
- What kind of surveillance? Targeted interception, bulk collection, hacking, device seizure etc.?
- Are the authorities allowed to share data from surveillance? If yes, with whom under which conditions?
- What procedures are used by the authorities to exercise surveillance?
- What crimes justify surveillance? Are there particular crimes that can easily be manipulated against people / organizations working in projects of international development?
- Are there safeguards, e.g. judicial warrants?
- What kind of oversight is guaranteed by law?

- Is there information on the technical capabilities of the state authorities, such as imported spyware from foreign (mostly Western) countries?
- Which authorities do you deal with and which authorities have an impact on international development's daily work? Pay attention to known risks and cases of abuse.
- Are there recent developments in the law to increase the collection of data, e.g. obligation to reveal passwords for accounts / devices?
- What are the legal circumstances under which companies have to provide data to governments, e.g. telecommunication service providers that provide support for phone interception?
- On what basis can foreign companies obtain data about their customers, e.g. Big Tech, like Google, Facebook, Twitter, etc.? Is there existing evidence that these companies comply?

### Helpful resources might be

- Laws of the countries, especially the ones governing secret and intelligence services, law enforcement entities and the police
- Transparency reports by both domestic/local and foreign-based companies
- Civil society reports by organizations with a focus on freedom of press, expression and/or the right to privacy





-  DWAkademie
-  @dw\_akademie
-  [dw.com/newsletter-registration](mailto:dw.com/newsletter-registration)
-  [dw.com/mediadev](http://dw.com/mediadev)
-  [akademie.dw.com/threatcheck](http://akademie.dw.com/threatcheck)

DW Akademie is Deutsche Welle's center for international media development, journalism training and knowledge transfer. Our projects strengthen the human right to freedom of expression and unhindered access to information. DW Akademie empowers people worldwide to make independent decisions based on reliable facts and constructive dialogue.

DW Akademie is a strategic partner of the German Federal Ministry for Economic Cooperation and Development. We also receive funding from the Federal Foreign Office and the European Union and are active in approximately 50 developing countries and emerging economies.



*Made for minds.*