# Keep what you need

The most basic rule for managing information securely is that any information that could put people at risk should always be compartmentalised and kept ?need to know?. This means that only those people who really need that piece of information to operate should be given it. For example, if a team is working with a high-risk source, only the source?s direct contact within the team should have his or her real name and details ? the rest of the team can operate using a code name. This reduces the risk for both the source and those other members of the team.

If there is not a good reason to keep a piece of sensitive information then you should simply delete it (see the [Safely Deleting lesson](umbrella://lesson/safely-deleting)).

# Threat Modelling

There is no single solution for keeping your information safe. Managing your information securely isn?t about which tools you use; it?s about understanding the threats you face and how you can counter those threats. To become more secure, you should figure out what you need to protect, and whom you need to protect it from. Threats can change depending on where you?re located, what you?re doing, and whom you?re working with. The easiest way to figure out what solutions are best for you is to carry out a threat modelling assessment.

# Assessment questions

When carrying out an assessment, there are five main questions you should ask yourself:

## 1. What do you want to protect?

What information could put you, your work or others at risk if were public? This is often the kind of information kept in your emails, contact lists, messages and files. It might relate to a specific sensitive campaign you are working on.

## 2. Who do you want to protect it from?

This could be any person or entity that poses a threat against an your or your work, also known as an adversary. Think about who would have a motive in reading or deleting your information or disrupting your work. Examples could be a government, a company you are exposing, your boss, or a hacker.

## 3. How likely is it that you will need to protect it?

It is important to distinguish between threats and risks. While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur. Calculating risk means figuring out the chance that a threat might actually occur ? how likely is it that a threat would be carried out? You also need to think about the capability of potential attackers. For example, your mobile phone provider has access to all of your phone records and therefore has the capability to use or share that data. A hacker on an open Wi-Fi network can access your unencrypted communications. A government might have stronger capabilities.

## 4. How bad are the consequences if you fail?

The motives of adversaries differ widely, as do their attacks. A company trying to prevent the spread of a video showing their illegal activity may simply want to delete the video, whereas a government may wish to gain access to the names/details of activists it sees as a threat to the state in order to arrest or harass them.

## 5. How much trouble are you willing to go through in order to try to prevent those?

This means figuring out which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about. Many people find certain threats unacceptable no matter what the risk, because the presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.

Swipe right for this lesson's checklist

### RELATED LESSONS

* [Safely Deleting lesson](umbrella://lesson/safely-deleting)

### FURTHER READING

* [EFF - Thread modelling](https://ssd.eff.org/en/module/introduction-threat-modeling)