ASSESSING RISKS

THREAT MODELING helps you identify threats to the things you value and who you need to protect them from. When building a threat model, you can ask yourself the following questions.

- What do I want to protect?

- Who do I want to protect it from?

- What are the consequences if I fail?

- How likely are these consequences?

- How can I address the most likely risks?

THREAT MODELING GLOSSARY:

Asset: What I want to protect
Adversaries: Who I want to protect my assets from
Threats: What are the potential consequences if I fail?
Risk: The likelihood that a particular threat against a particular asset will actually occur
Adversary capability: What an adversary is able to do to achieve its aim. For example, a country's security services might have the capability to listen to telephone calls while a neighbor may have the capability to watch you from their window. To say that an adversary "has" a capability does not mean that they will necessarily use that capability. It does mean that you should consider and prepare for the possibility.

Try it! Make a threat model for a jewelry store owner:

THREAT MODEL FOR A JEWELRY STORE OWNER

YOU inherit a JEWELRY STORE in the city.
The JEWELRY STORE has:

- $1 million worth of diamonds.
- A staff of five people.
- An alarm system.
- A safe.
- A cash register.
- A camera monitoring the door.
- A pin-protected alarm for the door.

1 **What assets are you protecting?**

- $1 million worth of diamonds
- Money in the safe
- Alarm code
- **Anything else?**

_____

_____

2 **Who are your adversaries?**

- Jewelry thieves
- **Anyone else?** (Consider: Who might have access to the jewelry store safe? What about cleaning crews, or maintenance staff?)

  Consider:
- What would motivate your adversaries?
- What are your **adversaries' capabilities**?

_____

_____

3 **What are the consequences if you fail?**

- Theft of jewelry
- Any other **threats?** (What if the safe code or alarm code is stolen?)

_____

_____

4 **How likely are these consequences?**

Map the likelihood of these threats occurring on the back!
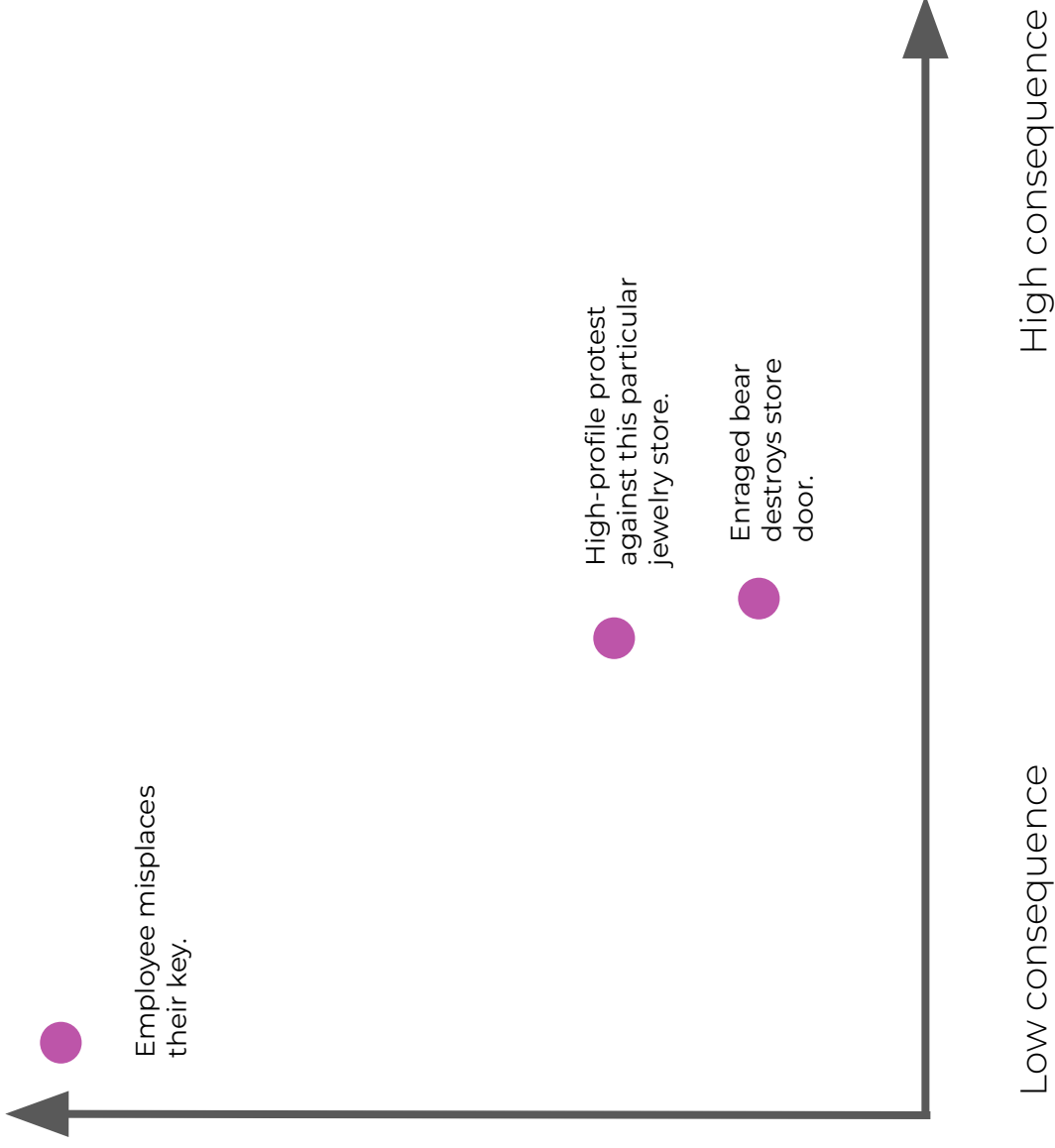
5 **How you can address the most likely risks?**

- Changing the passcode every month, and after an employee leaves.
- **What else?**

_____

_____

THREAT MODELING FOR A JEWELRY STORE

How likely are these consequences? This depends on your adversaries' **capabilities.**

Risk

High likelihood

Employee misplaces their key.

High-profile protest against this particular jewelry store.

Enraged bear destroys store door.

Low likelihood

Low consequence

High consequence

ASSESSING YOUR RISKS

1 **ASSETS:**

What do you want to protect?

_____
_____
_____
_____
_____
_____
_____

2 **ADVERSARIES:**

Who do you want to protect it from?

_____
_____
_____

What would motivate your adversaries?

_____
_____
_____

What are your adversaries' capabilities?

_____
_____
_____

3 **CONSEQUENCES:**

What are the consequences if you fail to protect those assets?

_____
_____
_____
_____

4 **LIKELIHOOD:**

Map the likelihood on the next page!

5 **PROTECTIONS:**

What kinds of protections make sense in response?

Fill this section out after completing #4 on the back. Determining appropriate measures depends on your appetite for risk.

_____
_____
_____
_____
_____

6 **PLAN FOR CHANGE:**

Technologies and threats change. Plan to reassess your risks.

I will reevaluate my threat model on: _____

Risk

High
likelihood

Low
likelihood

Threat