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:

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 can you 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.

- **Employee misplaces their key.**
- **Enraged bear destroys store door.**
- **High-profile protest against this particular jewelry store.**
# ASSESSING YOUR RISKS

A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
READ MORE ABOUT ASSESSING YOUR RISKS AT HTTPS://SSD.EFF.ORG/ AND HTTPS://SEC.EFF.ORG/

<table>
<thead>
<tr>
<th>1</th>
<th>ASSETS:</th>
<th>3</th>
<th>CONSEQUENCES:</th>
</tr>
</thead>
<tbody>
<tr>
<td>What do you want to protect?</td>
<td>What are the consequences if you fail to protect those assets?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>ADVERSARIES:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who do you want to protect it from?</td>
<td>What would motivate your adversaries?</td>
</tr>
<tr>
<td>What are your adversaries' capabilities?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>LIKELIHOOD:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map the likelihood on the next page!</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5</th>
<th>PROTECTIONS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>What kinds of protections make sense in response?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6</th>
<th>PLAN FOR CHANGE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technologies and threats change. Plan to reassess your risks.</td>
<td></td>
</tr>
</tbody>
</table>

I will reevaluate my threat model on: _____________