READ MORE ABOUT ASSESSING YOUR RISKS AT HTTPS://SSD.EFF.ORG/

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?)

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?**

5. **How can you address the most likely risks?**
   - Changing the passcode every month, and after an employee leaves.
   - **What else?**

Map the likelihood of these threats occurring on the back!
How likely are these consequences? This depends on your adversaries' capabilities.

- High-profile protest against this particular jewelry store.
- Jewels are stolen.
- Customer notices passcode to safe.
- Employee misplaces their key.
- Enraged bear destroys store door.

Risk

How likely are these consequences? This depends on your adversaries' capabilities.
## ASSESSING YOUR RISKS

<table>
<thead>
<tr>
<th>Step</th>
<th>Section</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ASSETS</td>
<td>What do you want to protect?</td>
</tr>
<tr>
<td>2</td>
<td>ADVERSARIES</td>
<td>Who do you want to protect it from?</td>
</tr>
<tr>
<td>3</td>
<td>THREATS</td>
<td>How would they threaten your assets?</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Map the likelihood of the threats on the next page!</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>What kinds of protections make sense in response?</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Technologies and threats change. Plan to reassess your risks.</td>
</tr>
</tbody>
</table>

**1. ASSETS:** What do you want to protect?

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

**2. ADVERSARIES:** Who do you want to protect it from?

**3. THREATS:** How would they threaten your assets?

**4. Actions:**
- Map the likelihood of the threats on the next page!
- I will reevaluate my threat model on: ____________

**5. Responses:**
- What are your adversaries' capabilities?
- What would motivate your adversaries?

**6. Technologies and threats change. Plan to reassess your risks.**
How likely are these threats? This depends on your adversaries' capabilities.