Modeling the Threats to Your Open Project

What threatens the stability of open projects?

About me

- Code for Science & Society
    - Fiscal sponsorship, strategic support of 6 projects
        - 1.8 million in total project assets
        - Grants, donations, fee-for-service work
    - Open Data, Open Source, Internet freedom, Open Scholarship, Open Advocacy

About this session

- 4:30 - me talking
- 4:40 - brainstorming and discussion
- 5:00 - threat modeling for your project
- 5:20 - share back, closing

What’s threat modeling?

- Worst case scenario time!

- “...potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized – all from a hypothetical attacker’s point of view…” wikipedia

- Identify threats
- Prioritize addressing them - which are most likely?
- (there are many types of threat modeling exercises)

My knowledge, blind spots

- Knowledge:
  - Operational, legal... boring administrative threats

- Blind Spots:
  - Technical security vulnerabilities

Threats (my experience)

- Legal status of entity, assets
- Financial management
- Governance
- Data handling, privacy
- Bus Factor

Legal status of entity, assets

- Who controls the assets (code repos, data, trademark)
- How are assets licensed?
- Is there an incorporated entity? (company, nonprofit)

- What's the threat?
    - Exposure to legal risk
        - licensing, disputes over ownership
    - Weird situations where project can't defend itself
    - Small projects = no budget for lawyers

Financial management

- What?
  - Who owns the bank accounts?
  - What is their formal relationship to the project?

- What’s the threat?
  - Money can literally get lost, disagreements over how money should be spent
  - Exposure to legal risk on tax, reporting, payroll issues
  - Small projects = no budget for lawyers

Governance

- Who makes decisions?
- Who makes *which* decisions?
- What is their relationship, responsibility to the project?

- What’s the threat?
  - No governance = no accountability, oversight
  - Inappropriate governance = complexity, slow progress

Data handling, privacy

- What data are collected?
- Where are they held?

- What's the threat?
  - Exposure to legal risk
  - Small projects = no budget for lawyers

The bus factor

- When one person gate-keeps an area of work

- What’s the threat?
    - If they leave, the project is in trouble
    -