Sara Brown
LFI – week 5
Example threat model // Instruction

Pt. 1: Example threat model

For: A child who fears for their safety if they are outed to their family

Assets

- Digital communication (emails, texts, relevant call history such as support hotlines)
- Browsing history
- Social media accounts
- Participation in online/in-person support groups
- Physical evidence (journal/diary, relevant books)

Adversaries

- Family members
- Peers who could reveal identity (intentionally/maliciously *or* unintentionally)
- Other adults in community (teachers/school officials, neighbors, friends' parents, coaches etc.)
- Data brokers/marketing firms (to avoid ads shown on shared devices about subject-based on browser history)

Consequences for failure

- Family: Kicked out of home, withdrawal of financial support
- Peers: Possible blackmail, harassment (intentionally); could tell family (intentionally or unintentionally)
- Other adults in community: Unpredictable – depends on outlook, relationship to child and family
- Data brokers/marketers: Could unintentionally provide clues to family

Likelihood of threats

- Family: very likely – Living at home, so family has many opportunities to discover assets even if they are not looking. Must consider intentional searches (e.g. checking browser history or installing spyware on phone) and unintentional discovery (e.g. finding book on subject in bedroom while cleaning)
- Peers: likely – Kids gossip and may not understand threat. Info must especially be protected from malicious peers
- Other adults in community: varies (dependent on specific individual/situation – for example, how often and in what context is the interaction? Teachers, coaches, friends' parents, neighbors will all have different levels)
- Data brokers/marketers: likely – extreme care should be taken with browsing history/device use on anything shared or potentially monitored

Measures to mitigate threats

- Private browsing on all devices
- Encrypt devices and all relevant files whenever possible (may not be possible for shared devices)

- Use code words in texts with friends (in case spyware/parental controls are installed)
- Multiple email accounts – one for general/public use (family members, unrelated online accounts) and another for any identity-related/private online activity (listservs, support group/message board logins). If possible, avoid using private account on home computer or any devices from school that are linked with real name/other personally identifying information
- Hiding spot for journal/diary and any physical items like books, and/or do not leave items in home (if feasible, though carrying items brings additional risks)
- Extreme selectivity in disclosing information to anyone, and emphasize danger to anyone who does know
- Avoid subject entirely, even in general terms, on social media

Pt 2: Instruction

Introduction to Threat Modeling

Threat modeling is a method of evaluating what information, people, or items are at risk, assessing who or what threatens them, and determining what steps you can take to protect against those threats.

This worksheet will guide you through the steps in creating a threat model. Each question has example answers to help you brainstorm.

Determine your assets: What do you want to protect?	*Example: online bank accounts, browser history, vehicle* ______________________________ ______________________________ ______________________________ ______________________________
Assess your threats: Who or what do you need to protect them from?	*Example: identity thieves, spouse/partner, break-ins* ______________________________ ______________________________ ______________________________ ______________________________
Likelihood of threat: How likely is it that you will need to protect each asset?	*Example: Do you use unique passwords for each online account? Are you in an abusive relationship? Have there been recent break-ins in your neighborhood?* ______________________________ ______________________________ ______________________________ ______________________________
Consequences of failure: What will happen if I fail?	*Example: How much time/energy will it take to recover your identity? Will you be in physical danger if your partner/spouse sees your browsing history? Do you have enough insurance to cover vehicle damage or theft?* ______________________________ ______________________________ ______________________________ ______________________________
Mitigating threats: What are you willing and able to do to protect against these threats?	*Example: Use secure passwords and a password manager, use a library or friend's computer to research shelters, park in a well-lit area/install a car alarm* ______________________________ ______________________________ ______________________________ ______________________________