The concept that “motives are a crucial mystery to solve”, is at the center of having good security. I hope to apply this with detailed logs for all security alerts I have come across. Instead of just noting technical facts like the attack method, I can take it a step further & record potential motives. An example would be asking if the attacker targets customer data for financial fraud, seeking intellectual property for profit sales, or just trying to disrupt everyday services. Reviewing threat intelligence reports around the web should help me narrow down the “why” behind some of the largest breaches that have happened recently.

For a new developer, it could be compared to securing a family home. You need to consider different intruders & their intended goals. A teenager might just be checking for an unlocked car in the driveway to grab spare change, which you prevent by cleaning your car out. A professional burglar, however, wants to steal high-value electronics and jewelry, requiring a robust home alarm system and safety. In the same way, if we are building a login feature, a hacker might try common passwords to hijack accounts for spamming, but if we handle credit cards, attackers will use more advanced techniques to steal financial data. Understanding these motives helps us choose the right defenses, like strong password rules or extra encryption.

Lastly, consider some cases of healthcare ransomware attacks. A recent case was the attack on DaVita & other breaches at various Texas Digestive Specialists. The initial motive seemed purely financial, as the attackers’ encrypted files and demanded payment. The hospital's IT team focused entirely on restoring systems and negotiating the ransom. However, a deeper forensic investigation revealed the true, hidden motive: the hackers had also silently copied thousands of patient records during the chaos. Their real goal was not just the one-time ransom but to sell personal information on the dark web for long-term identity theft and insurance fraud. This case shows how a surface-level understanding of motive can lead to a flawed response, causing the organization to miss the larger, ongoing data breach. It perfectly illustrates why digging for the real "why" must be a standard practice