Motive for possible attacks should always be considered as part of secure coding best practices. This is a crucial step for analyzing the threat landscape of any development project. Knowing what attackers want to do and why they might be motivated to attack helps a developer design code that is resistant to the anticipated attacks. In my practice I plan to consider the motive for attack as well as any likely avenues or flaws that may be exploited in the threat analysis phase. I will then work to minimize flaws that will allow the attacks to be carried out.

If I were explaining it to a new developer why this is important, I would compare it to defensive driving. Being aware of where a threat is likely to emerge from, like an intersecting street allows me to pay more attention to risks in that area, so I can do everything in my power to safely navigate through the threat.

An example I can use in module 8 is knowing attackers who are attempting to compromise a financial institution are likely looking to steal personal information such as account numbers and social security numbers from the institution. This allows the developers to ensure that data remains encrypted while stored, in use or while being transmitted. Using tools that support encryption especially while in use is therefore warranted for this data from potential threats.