Portfolio Reflection

Adopting secure coding standards and implementing secure coding throughout development of software is the best way to write secure code. By thinking of security from the beginning, you can plan how to structure the code in a secure way and while gathering requirements you can ask the right questions to understand the security needs of the software. Secure coding standards provide general practices to follow which will encourage consistency and establish expectations.

Evaluating the risk versus cost of mitigating security risks can help you prioritize security risk mitigations. If a risk is low priority, low threat, but would cost a lot to take care of, it would not be addressed as quickly as something that is high priority, high threat, and lower cost. By evaluating the risk versus cost, you can ensure that the higher priority security risks are handled first with the available resources.

Zero trust limits the chance of an internal security risk. By limiting permissions to the very minimum, sanitizing inputted data, and implementing authentication and authorization at multiple steps, you can decrease the likelihood of someone accessing data they should not have.

I recommend that security be implemented throughout the development of software. I also recommend that the secure coding standards are followed and maintained. It is also important to have a plan to mitigate breaches after they have already happened.