* Adoption of a secure coding standard, and not leaving security to the end

Adopting secure coding standards is foundational to implementing and communicating expectations amongst for security amongst the team. When we started this course, I was expecting a more detailed look into techniques, but I was surprised to find its more about relating what's important to everyone involved.

* Evaluation and assessment of risk and cost-benefit of mitigation

Case studies of the more modern breaches have left me with the understanding that its often more the people who are attacked in security breaches rather than the data itself, as many of these traditional attacks are pretty preventable.

* Zero trust

Zero Trust defines takes in to account that the more common attacks now are throught the employees and less the systems. So, things like phishing and scam-style attacks to gain access to passwords can be blocked by implementing a zero-trust approach, which requires re-engaging with security.

* Implementation and recommendations of security policies

Security procedures in today's society involve defending and resisiting attacks on staff as an accesspoint. So the defense against these attacks are staff training of scam tactics as they come up, varying validation of the staff identity at multiple points and stong layers of check every time a new one is made.