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

The software development teams often times miss to consider security at each stage of the development cycle and tent to think it is a task to be performed by the security team and keep it till the end. In my opinion, the security should be considered at each stage of the software life cycle – requirements, design, development and testing etc. The engineering teams should adopt the secured coding standards such as “validating all inputs” defined in security policy document. If it is not been done, anything discovered at the later stages not only costs significantly higher but actually delays taking the product to market. Depending on the severity of security defect, it could cause major design rework. On other hand, considering at each stage will give opportunity to discover earlier and remediate easily. Also, there is a huge miss perception with software teams that security is something belongs to security organization. In my opinion, everyone is responsible for security which includes business teams, architect, developer, tester and security team. If every person working on software understand the security policies and take care in each of their task, it helps to develop a most secured product.

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

Business teams run into this dilemma of risk vs cost benefit of mitigation. In my opinion, security is something can’t be compromised and it might lead to cancellation of business license. The way, I would think is “whether our application needs to be secured or not“. Security is something can’t be compromised, however there are techniques to lower the costs of security testing by adopting to secure coding standards and preventing security defects is less expensive than mitigation costs. One way to lower security costs is to have a good security policy, create awareness on the security standards with engineering teams, conducting security scans early phases of the software development and using automated test tools etc. The cost of the security testing can be significantly lowered with static security scanning tool usage, automated unit testing and other security testing tools etc.

**Zero trust**

Zero trust policy is a security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter. It is best approach to secure applications, networks and data etc. This course really helped me to understand security in depth by providing data breach examples and how organizations suffered. I feel more confident in speaking about the importance of zero trust policy and influencing the leadership teams. Enhancing any security policy may cause change to user experience and frustrate users if not designed intuitively. For example, replacing user login procedure of entering userid & password with biometric authentication (Face Id and Touch Id) will actually simplify the user experience and enhance the security. Hence engaging the designer is critical while enhancing security policies that would impact user experience. I will be able to persuade developers in better with the knowledge gained through this course. Especially, using the examples of organizations that suffered due to security breaches and business impacts etc. Also will pay attention to cause of resistance such as increased effort and influence leadership teams on the investment required to implement zero trust security policy.

**Implementation and recommendations of security policies**

Every organization should have a security policy with secure coding standards, procedures and automation tools etc. Adoption of security standards and security testing should become part of the culture. The engineering teams should be given required capacity to implement and adopt the security practices otherwise adoption would be failed. To provide efficiencies for engineering teams, security scanning tools should be adopted and integrated with IDEs.