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

Security should not be an afterthought. Preventing attacks must be done in advance through testing, researching the latest security trends and how teams can design and implement code to prevent against threats. This happens throughout the lifecycle whenever possible. Team members must have the attitude of protecting data, employee and customer information at the forefront of their minds. The prevention of vulnerabilities during the build of software products.

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

Evaluation and assessment of risk can be completed through static coding analysis tools, research of common threats and vulnerabilities hackers tend to exploit companies and individuals for, lastly common developer logic errors created to prevent against specific attacks and vulnerabilities. Always test code for logical and functional errors. Code defects can happen up to deployment and afterwards. Preventing cyber-attacks and enhancing vulnerabilities means, practicing the best standards must always be a high priority. One may write a function to throw an exception, when necessary if an input exceeds 10 characters, the program will notify the developer. Some benefits of prevention include saved revenue, the safeguard of data, and company integrity.

**Zero trust**

Zero Trust enforces the culture within companies to maintain an attitude towards safeguarding data, information of customers, and employees, also, physical items such as hard drives, or removeable drives. “Trust no” one will help in keep companies safe from unwanted data breeches or thievery through the internet, physical breeches such as penetration testers, or any unauthorized and unauthenticated person wanting to gain access to a restricted area. Weather over the internet or in person. We must keep the wrong people out. How we maintain this is by verifying everyone.

**Implementation and recommendations of security policies**

The implementations of security policies are a must have to keep and ensure safety of company data, recourses, assets, stakeholder data, and of course, employee information. The recommendations of security policies are also another important use case within secure coding best practices. The reason behind this is to prevent attacks and vulnerabilities, developers and other team members must collaborate to ensure any weaknesses within the design infrastructure and code base are rectified. The weaknesses may include, defective code, bad naming conventions, uncommented code.

This can make interpreting the code harder. Developers may encounter problems of different languages and will need to quickly decode, interpret, and debug if need be. This within itself can be in my future security policy “always comment your code and use proper naming conventions”. To take it a step further, I may include another standard called “security not last, it must not be an afterthought”.