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

As a company deciding on a secure coding standard and sticking to it will greatly benefit you. Overall, it will make sure things are uniform as well as help with future maintenance of the overall application. A secure coding standard will ensure that the developers of the application will follow a predetermined set of rules and guidelines rather than the programmer’s familiarity or preference. Security comes into play during the design and the implementation phase of the project. With security, you are only as strong as your weakest link. With this being said, there are multiple things you can implement to ensure the application is being covered with the defense in depth methodology.

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

When evaluating and assessing risk along with cost benefit of mitigation, I would need to run static analysis testing tools to find common vulnerabilities that exist within the code. When vulnerabilities occur, I would run a deep dive research and configure an approximation of cost if they go unfixed. Then I would project a cost of how much it would be to mitigate the vulnerability. Once the weak points are found within the application, examine the priority and likelihood of the specific vulnerabilities. This would determine the importance in which they are to be mitigated.

**Zero trust**

While hackers only continue to get smarter, we need to improve our code as well as our tools to remain protected from potential threats. In today’s time, attacks on Common Vulnerabilities (CVE) are continuous and constant vigilance is crucial to keep your application protected. These CVEs need to be checked and tested vigorously. The system needs to trust no one and verify everyone. The verification process happens multiple times to ensure the user is who they say they are. With this policy, there are Five pillars to implement when transitioning to a modern model such as, Device Trust, User Trust, Transport/ Session trust, Application Trust, and Data Trust. These pillars are essential to provide security organization with a holistic platform-based approach that intertwines context from devices, users, applications and more. With the implementation of these five pillars, we are able to gather analytics across the digital environment.

**Implementation and recommendations of security policies**

If I were to make implementations and/or recommendations to security policies, I would include a cost prediction. This prediction would include a diagram that would show what it would look like if the company were to implement it. I also believe that there should be a diagram on the cost if someone were to access the critical information, and how much it would cost to get the company back on top. These diagrams would be compared to explain what the best course of action should be when it comes to security. Another thing would implement in the security policy is a timeline. The reason for this is that it would provide an insight into how often the company needs to update the lifecycle of the security standard that was followed, and what it would entail. These could be things such as checking for newfound CVEs as well as updates to the system to improve security overall.