Having a set of secure coding standards is a proactive approach to cyber threats. Where these security standards become an integrated part of development from the beginning rather than after the fact. This ensures the applications are secure against known vulnerabilities and overall lowering the chances of a security breach. And reducing the chance of an expensive set of costs to fixing the application and possibly repairing any reputation that was harmed.

The evaluation and assessment of risk along with the cost analysis is a crucial step in determining the best strategy. This process starts by identifying potential threats and motives, assessing the likelihood and impact of each, and then the best and cost effective way to mitigate them. Cheaper is not always better when it comes to security. But instead of understanding the pros and cons between the cost and risk you can properly allocate resources to make a better informed decision about security.

And Zero trust should also be considered as its a model that operates on the model of “No one is safe”. Having an approach like this assumes the threat can exist not only from the outside, but from within the company as well. Having strict verification processes and re-verification every so often while having DiD layers can significantly reduce a security breach. At times it can be overlooked as you are trying to prevent a sophisticated attack you often forget the person behind the attack can possibly be stopped by having zero trust in place.

And lastly the implementation and recommendations of security policies should overall be tailored to each organizations needs. Along with that, policies should not contradict each other, they should be clear, and comprehensive to the people that are implementing them. All while protecting critical information that the company may have. And the biggest vulnerability to any cyber threat is the user themselves. So training should be an important factor as human error is a significant cause for these breaches.