Adopting a secure coding standard is absolutely necessary to any company or project that does not wish to be completely open to hackers. Software is not just intrinsically secure and wishing it to be safe without setting in place a standard to actively guarantee security will only result in heartache. In that same vein, security should never be an afterthought. Security should be considered from the very beginning, and it should be woven into every part of the life of the software. Doing otherwise is just another recipe for disaster.

In order to address security vulnerabilities, one must be able to diagnose risks. These are accomplished through risk assessments. Once these assessments have been performed, it is now possible to anticipate and plan for the steps that will need to be taken to mitigate these risks. The cost benefits of mitigating security risks are enormous, but they can be unfortunately difficult to give an exact number. Mitigating risk is an inherently preventive process. The amount of money that would have been lost by having data stolen, the system down, reputation lost, and credibility dashed is never known until the vulnerability is exploited. Nevertheless, the potential loss of money from risks can be very large, and therefore it is best to consider risk mitigation as a very beneficial practice.

Zero trust is a policy of giving exactly no trust to anything as a standard. Components of a system, networks, users, databases, devices, and many more aspects of a system all treat every exchange as risky. Following this policy ensures that it is nearly impossible for an attack to make it past enough levels of security to get anywhere. It is an extremely stringent policy that may take a lot of work to implement, but it is the most logically secure.

Implementation of security policies should be universal across an organization. Attempting to change the way things are done overnight is not a good practice either. It is best to roll out large changes over a period of time. This allows people the chance to get trained and adjust before the policy becomes required. There is no such thing as a perfect security policy, so it is best to keep an open mind, study up on the latest technologies and cybersecurity tactics and attacks and adapt the policy to keep up with the ever-changing tech landscape.