Throughout this course, I have been able to gain an appreciation for the importance of integrating secure coding standards into the software development lifecycle from the beginning. Adopting standards, such as the SEI CERT C++ Coding Standard (SEI, 2024), early on, developers are able to address potential vulnerabilities proactively, overall reducing the chance of security breaches. Taking this approach aligns with the idea that security should not be an afterthought but instead a fundamental aspect of the development process. Implementing these types of measures from the start not only improves the overall integrity of a system but also saves potential time and resources that would have been spent to fix vulnerabilities found much later down the line.

Evaluating and assessing risk is a core part of developing a secure system. Thoroughly analyzing potential threats and the costs associated with them can inform organizations into making smart decisions about which security strategies should be employed. An important aspect of this process is to consider how malicious actors think and what motivates them. For example, are they attempting to secure a large amount of personal data through a scraping operation, like in the case of the 2021 LinkedIn data breach (Baek, 2023)? Or do they want access to an account that doesn’t belong to them? Each case requires a different security measure, which should all be implemented as several layers. Utilizing multiple layers of security is known as defense in depth and is the idea that if one layer fails, another is still in place to keep the system safe.

The implementation of a Zero Trust model changes the traditional perspective on security by removing the assumption that any use or device is trustworthy by default. Instead of relying on the credentials or local network location as trust indicators, taking this approach requires continuous verification for every access attempt. This means that security inherently becomes a more active and dynamic process, bringing both constant authentication and authorization to the forefront. For users, this has the possibility to introduce additional steps like multi-factor authentication (MFA), which introduces a slight hinderance to routine operations. It is important to note that despite this inconvenience, the enhanced protection of sensitive data makes the approach worth it.

Finally, the development and implementation of robust security policies is an essential step in maintaining a highly secure system. These policies provide clear guidance to all members of the team for ensuring data is safeguarded and legal requirements are fulfilled. The recommendations for security policies often include regular staff training, routine security checks and assessments, and creating plans for responding to different incidents. By establishing and enforcing these policies, an organization-wide culture of security awareness and accountability can be developed over time.