**Portfolio:**

Perhaps, protecting the security of either an app or business is first and foremost duty of a developer. But sometimes we put security over other things. For example, while developing an app, we have used sources and log in/ sign up, if the data has no protection in database against threats, then the data of users are at threat. In the phrase, “Don’t leave the security to the end”, it means solving the security threats from leaking data is more important than other tasks. Thus, this phrase simply focusses on the security of user’s data.

There are various steps such as, restrict access to sensitive data, Limit administrative access, Store passwords securely, Guard against brute force attacks, Keep sensitive information secure throughout its lifecycle, Use industry-tested and accepted methods, Ensure endpoint security, Put sensible access limits in place, Verify that privacy and security features work, Test for common vulnerabilities, Put it in writing, Securely store sensitive files, Dispose of sensitive data securely, etc. These steps are the basics of every security, if these preventions are taken, the app or business will likely to be at lower risk.

The factors like time, money, reputation and operations are more to consider a program requires a lot of time to write. For big organizations and companies, writing a secure program also cost a lot of money. As mentioned in the book, the organizations that been exposed to cyberattacks have lost their reputation such as, “The 2010 CyberSecurity Watch Survey, conducted by CSO magazine in cooperation with the U.S. Secret Service, the Software Engineering Institute CERT Program at Carnegie Mellon University, and Deloitte’s Center for Security and Privacy Solutions [CSO 2010], revealed a decrease in the number of cybercrime victims between 2007 and 2009 (60 percent versus 66 percent) but a significant increase in the number of cybercrime incidents among the affected organizations. ……...Of those who experienced e-crimes, 25 percent reported operational losses, 13 percent stated financial losses, and 15 percent declared harm to reputation as a result. Respondents reported an average loss of $394,700 per organization because of e-crimes” (eBook). The online fraud and attack also result in loss of millions of dollars.

Well, this model really aligns with Device, User, Session, application and data. Well, my concepts are entirely changed when i first read about Facebook and its security. After researching by time, i feel we are not safe at all in this advance era. Smart phones are tracking system, our personal information can be leaked at any time. Moreover, no one is safe since we are giving permission to the apps to track us. As a user, I stopped putting any personal information on social media accounts, but as a content creator i tried to post every professional information. Every developer should know the basics of zero trust, so they can better judge and provide their decision.

* Do not modify constant objects
* Do not attempt to modify string literals.
* Prevent SQL injection
* Detect and handle memory allocation errors
* Never use assertions to validate method arguments