Defense in Depth is a way to deal with network safety. When writing code, the programmer should be cautious of systems being layered to secure vulnerable information and data. It’s kind of like a failsafe as one event falls flat another can move in and replace the previous failed event without throwing any errors. The tradeoff to this way to deal with network safety is your anticipation of these vulnerabilities brings less issues with code later.

An attack on your network could cost you a great deal of time finding the errors which allowed a back door entry. By using techniques to mitigate this while writing code you can save you and your company a time. During these entries money can be lost in forms of account information being accessed. When these attacks happen, your reputation could also be on the line in from losing customers to an overall trust from your client relationships. Lastly, if databases contain information confined to restrictions from legal laws you could incorporate fines, lose of licenses, and regulation ending up in operational considerations.

DiD (Defense in Depth) ensures a standard of protection from attacks. It consists of things like Fix Management which is a way to apply updates to working framework, programming, and equipment. Firewalls to ensure IP addresses are not left out for external access.