* **How deep is too deep, and what’s the tradeoff?**

Before we can say how deep is too deep, we first must know what defense in depth is. Defense in Depth (DiD) is a cybersecurity approach that uses multiple layers of security to safeguard a network, web resources and other network connected assets to prevent attackers from accessing those assets.

There is no one size fits all when discussing any kind of cybersecurity, attackers get smarter and discover new techniques to break security. With that being said, I don’t believe there is a clear answer for how deep is too deep. I believe the answer will change depending on who is asked that question, a cybersecurity person may say you can never go too deep whereas a developer may have a different answer.

There is a delicate balance between enough security and the performance issues caused by the security policies set forth by a cybersecurity department. A major tradeoff works in one of two ways. Too much security and end users will suffer, and too little security may result in an attack. There must be a clear decisive plan for keeping security as high as possible with a little impact to end users as possible.

* **What are some time, money, reputation, and operational considerations?**

I currently work for a very large company in which I provide technical support for employees. The company puts security above its end users which results in end users spending more time fighting against security policies and mechanisms set forth by cybersecurity that it affects productivity. When security policies are preventing end users from being productive it is costing the company money and time.

There must be a balance between security risk versus performance. I know attacks costs lots of money and time to recover from should an attack be successful. Reputation is two-fold, if the reputation of the company is that end users cannot work due to security policies potential employees may choose to not start working. On the other hand, if an attack takes place, it will be may potentially be made public which could affect future business. It could cause a loss of clients, deals or suppliers. Operational considerations could result in fines or other penalties depending on the cause of an attack.

As mentioned above, it is very delicate when considering money, time, reputation, and operational considerations whenever discussing any kind of cybersecurity, not to mention defense in depth. Too much security and user productivity could be impacted costing the company money, time, and reputation. Too little security and the company could suffer a successful attack costing the company money, time, reputation, and other operational issues.

* **What are some additional aspects of DiD that make it unique for each situation?**

Aspects that can make DiD unique for each situation I would say company structure, environment, networking hardware and endpoints. Things like do all workers work remotely, do all workers work onsite, is there a mix of remote and onsite workers, are there any workers located outside the continental U.S. all could affect DiD. Firewalls have a major impact on DiD because they are one of the layers in security. Another aspect that can be unique for situations is endpoint security, how patches are delivered, up-to-date software, password policies and other security mechanisms are unique as well.