1. VLAN/Subnet Segmentation

Importance: Whenever you make a network from scratch you always want to split up segments within the network to improve security, speed, and scalability. Having everything under one big network does not do well because everything is clustered together, troubleshooting becomes even harder, bandwidth speeds fluctuate, and it is hard to apply any ACL/firewall rules to have a security layer between the different departments within a company.

Real world situation: VLAN/Subnet segmentation is very important especially in startup companies that are looking to expand over the years. It allows you to divide up a network address that is given to you using VLSM. Say a company has 4 departments HR, Finance, Engineering, and Call center. You don't want Call center people to access any sensitive information from Finance like tax pay rolls or contracts, so what do you do? You separate Call Center and Finance using VLAN/Subnet segmentation and put ACL rules to stop all communication between those departments. That is just one scenario but the general rule is to always separate your departments into different VLANs/Subnets in order to better maintain your network infrastructure.

2. Internal and External WiFi Networks

Importance: Any large company with an extensive network infrastructure is bound to have wireless access points to allow IoT to access the network. This neat thing called WiFi is the best thing to happen to the world but does provide security flaws just like anything in this networking field. That is why it is important to segment your wireless networks just as you would with an internal network. IoT can provide many benefits that come in the form of security cameras, printers, smart TV's, etc but the device itself has security flaws that are not in the control of the networking team but the manufacturer. Segmenting your wireless networks allows your IoT things to access the network infrastructure without compromising your data. If the IoT was to get hacked then the hacker would have no access to your internal network infrastructure since it is not part of the internal network but part of the external infrastructure.

Real World Situation: Having an internal and external WiFi network benefits startup to medium sized companies where they might not have the funds to purchase state of the art security technology. They rely on rundown technology that may come with security flaws straight out of the box but having an internal and external WiFi network allows that extra layer of security. Say for example the company installs security cameras that require internet connection, instead of connecting it to the internal WiFi network the company can make a separate WiFi network that has no ability to communicate with the internal network but the internal network can fully communicate with the security cameras. This allows the networking team to be in full control of the infrastructure while mitigating security flaws that the manufacturer presents.

3. Sandboxing

Importance: As a company you never want to be stagnant because as technology advances everyday so do hacking tools. Every company needs a department that experiments with patches and security updates. With this being said though you don’t want to experiment with the actual network infrastructure that is in use because if a security protocol was deployed and was not to work it can affect the workflow of a company. That is the last thing you want within a company. Not only does sandboxing help with patches and security updates but also allows you to study any applications that you may want to deploy and even reverse engineer any malware to improve upon your security. There are many benefits that sandboxing brings to the table within a company.

Real World Situation: There are many cases where having a sandbox environment within a company is just as necessary as segmentation. Companies love updating to the newest patch of every application they use to better secure their end users but sometimes those patches come with problems that are not seen at that moment but come to fruition in the future. Sandboxing allows the company to test out the newest patches before they are actually deployed to the network. This saves the company a headache that can occur if the patch was just deployed without testing how it will affect the end users.