The NIST could provide outlines for companies to address cyber situations in a more organized manner. Being able to have step-by-step guidance makes it easy for anybody to adapt to the policy and provides for more flexibility. The different aspects of NIST from identification to the recovery phase, having this in effect helps the company as a whole save funds. As the majority of the time these companies only care about the financial impact it may have on their economy. Now with that being said, this outline is very broad and you could possibly go into way more detail than the 5 phases themselves. I feel like this will become more valuable as I get more experience in the field when I get access to those more administrative cyber roles. I could always suggest this to my boss at the time or use it personally to address a situation. Being able to use this to enforce a policy into a system would be fantastic but it'll take time to be able to reference, kind of like wine that ages well. Overall it's a framework that is universal in most lines of cybersecurity work, where most of the time it will have some type of impact on how we address problems