In the cybersecurity sector, things change so rapidly and so drastically that certain policies and infrastructure must be utilized and kept updated, but because of the “short arm” of “predictive knowledge”, these additions or improvements typically are added as a reaction to an event, not before the fact. If a proactive approach was taken using predictive knowledge, the data is not currently reliable enough to guarantee it would be effective. This could lead to wasted policies or wasted upgrades to infrastructure, wasting money, time, and effort. Due to this, the reactionary approach is currency used by most companies. This reactionary approach that the cybersecurity industry has been using would be far outclassed by a proactive approach, however due to the lack of ability to accurately predict changes in the cybersecurity field, the reactive approach is what is currently used. This is a very bad thing, and if predictive knowledge was better, enough so that additions wouldn’t turn out to be pointless, then the amount of vulnerabilities in a system would decrease far faster than they are now. Unfortunately, the cybersecurity sector is so volatile and everchanging that such knowledge is not truly reliable right now, and so the current reactionary approach is unfortunately the best we have at the moment. This is the correct way to go about things, until predictive knowledge improves drastically in cybersecurity, in which case these additions should be made as soon as they are known about. Improving predictive knowledge should be a major goal of many cybersecurity specialists, as when it improves enough to be reliable, cybersecurity will be much more effective overall. Hopefully, in the near future, predictive knowledge will be reliable enough to be utilized on a grand scale, which would lead to a more proactive approach to cybersecurity, rather than the reactive approach used today.

Jonas, H. (1973). *Technology and responsibility: Reflections on the ... - JSTOR*. JSTOR. Retrieved November 27, 2021, from https://www.jstor.org/stable/40970125.

Dickson, B. (2018, March 16). *How predictive analytics fights the cyberthreats of the future*. TechTalks. Retrieved November 27, 2021, from https://bdtechtalks.com/2016/07/13/how-predictive-analytics-fights-the-cyberthreats-of-the-future/.

Hi Jeremiah
I agree that the use of predictive knowledge should be a factor in designing more policies and better infrastructure, but not on a massive scale. The reliability of predictions in the cybersecurity field is just not great enough yet to make entire policies or infrastructure out of. We should be looking to mitigate the obvious threats to cyber systems right now, not predicting issues that could not yet be relevant. Having said that, at what point should we start relying on predictions and take a more proactive approach?