NICE Frame Work

The NICE framework is made up of different areas in cybersecurity and they are the following identify, protect, detect, respond, and recover. These all have important roles they accomplish but when they are all paired with one another they create a design that many companies and businesses need to strive for. It is a system that can applied to nearly all cybersecurity incidents. It allows you to see an issue, what to do with it, and then how to recover. Since there are many areas in this framework, I would choose to target one or two areas that I would want to focus my career on. Those are identify and detect these prevention systems work hand in hand with one another. These stick out to me because it allows you to be one of the first responders when it comes to computer operation. Needing to identify issues on a computer allows you to do continuous scans and file research. Detection is a key part of the framework being able to target a problem before it snowballs into a catastrophic event. As stated, before they work very well with one another so these would be the most interesting to focus on. The areas that would appeal to me the least in the NICE framework are respond and protect. Having prevention systems like malware protection, anti-virus, and firewalls is a great way to see in what ways are needed to protect or respond. These areas are crucial in the framework like the rest but they do not give off the same interest as the other ones. All of these areas of the NICE framework when combined are a great tool not only businesses and companies need to use but by everyone.

WordPress link:

https://sites.wp.odu.edu/clarencekimbrelljr/2022/01/20/interests-in-the-nice-frame-work/