

Reflection Paper 3

Amari Fisher

11/09/2025

Third Reflection

After completing 150 hours of the cybersecurity internship provided by COVA CCI, I have learned the importance of frameworks and standards when it comes to cybersecurity at an organizational standpoint. During development of our presentation, we utilized both CIS benchmarks and NIST CSF to conduct our formal analysis of Suffolk's overall cybersecurity posture and their sql servers window systems compliance. CIS benchmarks in particular is a very important standard in our analysis because it is the one of the standards that are directly integrated into Tenable, and backed by tenable to ensure proper compliance of end systems. Compliance scans find things such as configuration issues that would be overlooked by pure vulnerability scanning because these issues aren't necessarily attached to an exploitable vulnerability. However, the power in these issues lies in the fact that no system can be completely protected from every possible vulnerability, so when compromise eventually happens, you should attempt to make it as difficult for the exploiter to move around as possible, and make it so that the exploiter can not easily move on to access the more critical systems from any particular endpoint on the network. Whether that's through properly configuring admin account password resets, or disabling certain system settings, the point remains the same.

NIST Mapping

Although NIST CSF isn't explicitly integrated within the city of Suffolk, besides them understanding the basic principles and applying it to their organization. NIST CSF was one of the more important frameworks that we've used when forming our presentation and powerpoint

because it allowed us to map the current systems that Suffolk already had in place to the specific families within the NIST CSF.

Conclusion

In conclusion, frameworks like NIST CSF and CIS help to provide baseline standards to any organization, no matter the size or scope of the organization. The usefulness of both frameworks are reliant on the task. The NIST CSF would serve well as an organizational baseline framework, and would be very useful in high level scenarios that focus on the executive side of cybersecurity, while the CIS framework provides for direct analysis with their benchmark that directly maps toward the lower level compliance and technical sides of cybersecurity.