Fougnigue Sefon

CIDM 6395

Assignment 2: Assessing Networking and Cybersecurity

As I near the end of my studies in Computer Information Systems and Business Analytics, it's important for me to look back at what I've learned, especially in Networking and Cybersecurity. This reflective appraisal serves not only as a testament to my growth but also as a blueprint for my future learning trajectory.

What I Know: My Areas of Strength

My coursework has equipped me with valuable skills and knowledge across various aspects of cybersecurity. Notably, I've become proficient in conducting vulnerability assessments, understanding the intricate processes of data deletion and recovery, creating contingency and audit plans, and understanding the legal and ethical issues in computer security.

Conducting vulnerability assessments has taught me how to systematically identify, rate, and recommend fixes for vulnerabilities in a system, which is essential for preventing security breaches. The complexities of data deletion and recovery have shown me that ensuring data is securely erased or recoverable in disaster scenarios is not as straightforward as it may seem, requiring a deep understanding of how data is stored and can be forensically retrieved.

Additionally, my ability to create comprehensive contingency plans means I can effectively prepare for and respond to incidents to minimize their impact. Developing audit plans has also been a key strength, allowing me to systematically review and improve security policies and practices.

Moreover, the exploration of legal and ethical issues has prepared me to navigate the complex legal landscape and ethical dilemmas that arise in the field of computer security, ensuring compliance and promoting ethical conduct.

These areas combined with my knowledge of common attacking techniques position me strongly within the field.

Where I Am Weak: Areas to Improve

Despite these strengths, I recognize areas where my knowledge and confidence are lacking. My understanding of cryptography is also less robust than I would like, with the technical details of implementing cryptographic solutions remaining elusive.

Furthermore, my knowledge of cloud technologies and security is limited. As cloud computing becomes increasingly integral to the infrastructure of modern businesses, my lack of familiarity with cloud platforms, security strategies specific to cloud environments, and best practices for cloud-based data protection is a significant weakness.

Moreover, the dynamic nature of cybersecurity demands constant vigilance and learning. Staying informed about the latest trends and threats is a difficult task, yet it is crucial for a cybersecurity professional. My current approach to continuous learning in this fast-evolving field needs to be more structured and proactive.

Future: How I Plan to Grow

To bridge these knowledge gaps, I intend to pursue practical experience, particularly in projects. Specialized courses or certifications in cryptography and cloud security could also help in deepening my understanding of these complex areas.

Committing to continuous learning is essential for staying current with the latest developments in cybersecurity. This will include engaging with industry publications, joining professional networks, and attending conferences or workshops.