8-2 Cyber Playbook Submission

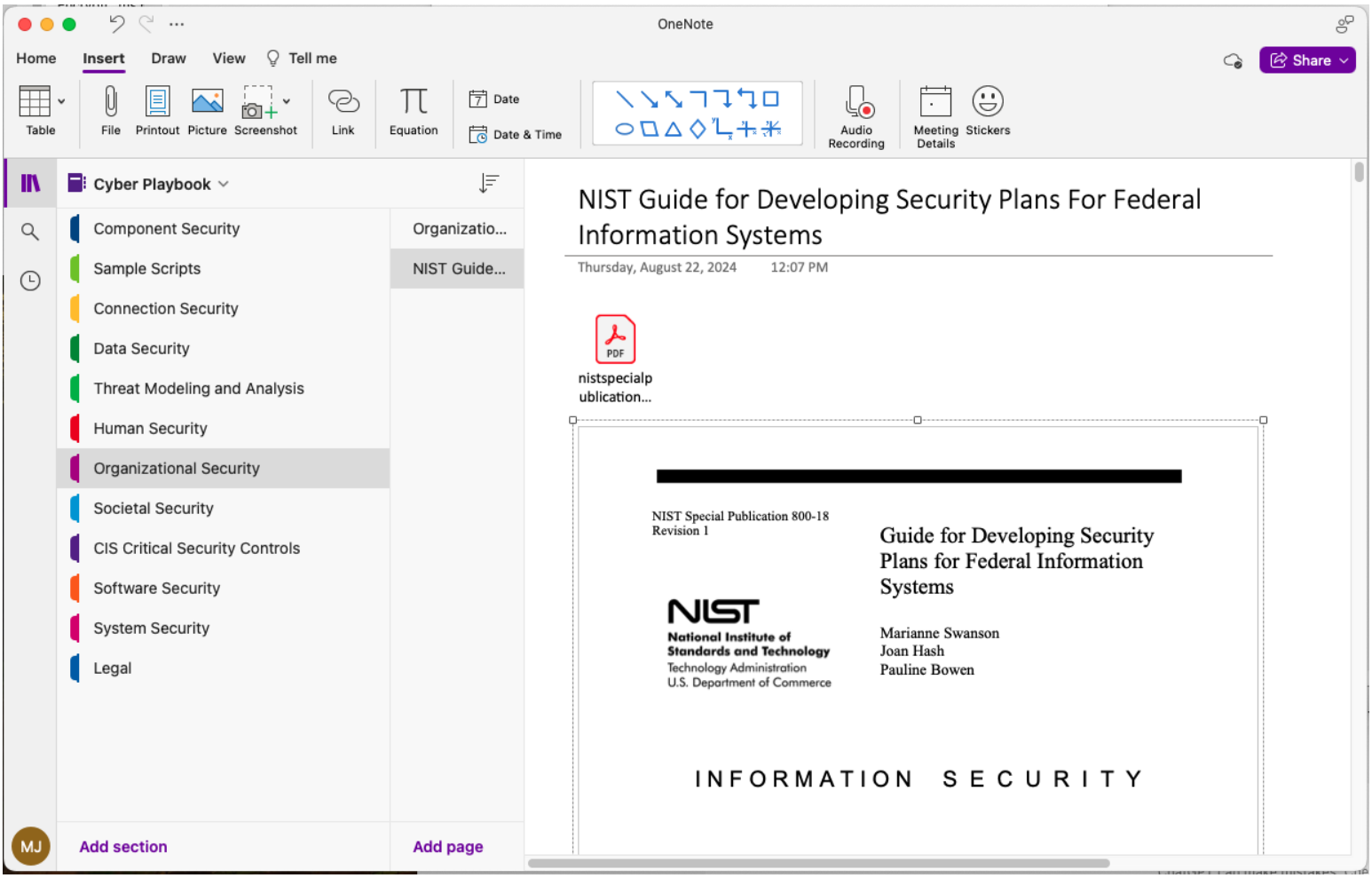
Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

22 August 2024



The section from my cyber playbook on the "NIST Guide for Developing Security Plans for Federal Information Systems" is the most helpful part for me, both for now and for my future career. This guide teaches how to set up security plans that meet government standards, which is crucial because these systems hold susceptible data. For instance, consider a scenario where a federal agency faces a data breach, compromising sensitive health records. By applying the principles outlined in the NIST guide, the agency could have ensured that proper access controls and encryption were in place, potentially preventing such a breach.

Understanding the NIST guide helps me see the big picture of cybersecurity. It shows how to protect information and why it is essential to improve these protections. This knowledge is something I can take into any job in cybersecurity, making sure that the systems are not only defending against current threats but are also ready for future challenges. As new forms of malware or cyber-attacks emerge, the strategies from the NIST guide could help an organization develop proactive defenses, ensuring consistent protection of sensitive information according to the latest security practices. This part of the playbook prepares me for real-world situations where I must apply these principles and ensure I know how to handle sensitive information correctly.