Ava McLaughlin

CYSE200T

February 27, 2025

Special Guest Speaker Mr. David Price

BLUF: Mr. David Price, an experienced representative of CISA (Cybersecurity and Infrastructure Security Agency), shared many helpful and interesting insights during Tuesday's class. Three of them that stood out were CPG's, OT, and national threats.

The primary topic of Mr. Price's discussion were CISA's Cross-Sector Cybersecurity Performance Goals (CPG's). These are goals that serve as a baseline for all businesses when implementing cybersecurity practices but are particularly helpful for medium or small businesses. Cost, impact, and ease of implementation are factors used to determine which goals to implement first, helping businesses prioritize their efforts and distribute resources effectively. CPGs do not impose regulations, and CISA offers free evaluations to help businesses assess their cybersecurity frameworks.

Another interesting topic Mr. Price discussed was OT (Operational Technology). Unlike Information Technology (IT), operational technology manages physical processes. When most people, including myself, think of cybersecurity, they often focus on IT and online security threats. However, attackers have exploited this mindset by infiltrating systems through OT. Mr. Price uses the Colonial Pipeline attack as an example of the vulnerabilities in OT, where attackers infiltrated the system, deployed ransomware, and shut down the network, causing a fuel

shortage on the East Coast for several days. OT is particularly vulnerable because these systems were not designed with security in mind and are difficult to replace.

The last intriguing topic was Mr. Price’s comments on national threats. CISA is part of the United States Department of Homeland Security (DHS), which focuses significantly on addressing foreign threats. Additionally, Mr. Price's experience in Navy, Army, National Guard, and Air Force intelligence provides him with broad knowledge of the evolving strategies of foreign attackers. He mentioned Salt Typhoon, a sophisticated Chinese hacker group focused on stealing information rather than disrupting systems. Another example of dangerous foreign threats is the very recent North Korea Bitcoin theft, where they successfully stole approximately $1.5 billion USD from Bybit. Mr. Price’s discussion on the vulnerabilities in American infrastructure made me realize just how sophisticated and dangerous foreign attackers can be.

Conclusion: Mr. David Price's discussion displayed noteworthy cybersecurity concerns, including the importance of CPGs, the vulnerabilities of OT, and the growing threat of foreign cyberattacks. He stressed the importance of businesses and infrastructure enhancing their security practices to address these evolving risks, a goal he is helping advance through the anticipated release of CPG 2.0 in August 2025.