Margie Owusu

Jospeh Asmus

Department of Treasury

CYSE 368 Fall 2023

November 30, 2023

Internship with The U.S. Department of Treasury

This paper provides a comprehensive overview of my internship at the U.S. Department of Treasury, an experience that spanned of three months from September to December 2023. As an intern in the departmental office, in their threat intelligence team. I was afforded a unique and enriching opportunity to contribute to and learn from one of the most pivotal financial institutions in the United States.

The role I undertook involved, assisting in the analysis of threat groups trends, and supporting policy development related to national economic security. My responsibilities were multifaceted, encompassing both collaborative and independent projects, and allowed me to apply my academic knowledge in a practical, real-world setting. This engagement not only enhanced my understanding of the Treasury's operations but also provided valuable insights into the intricate workings of federal monetary management and policymaking.

The purpose of this paper is to articulate and reflect upon the experiences, learning outcomes, and professional development acquired during my internship. It aims to dissect the application of academic theories in a practical environment, analyze the skills honed, and evaluate the overall contribution to and impact of my role within the department. Furthermore, this paper serves as a synthesis of how this internship has shaped my perspective on a career in government service, particularly in the realm of finance and

economics. Through this reflection, I endeavor to provide a detailed account of my journey, the challenges encountered, the triumphs celebrated, and the invaluable lessons learned along the way.

The Treasury's commitment extends to proactively identifying and countering cyber threats that could undermine national economic stability. This involves collaboration with other government agencies, private sector partners, and international allies to gather and share critical intelligence. In fulfilling this mission, the integration of threat intelligence becomes essential. This involves continuously monitoring and analyzing cyber threats and vulnerabilities to protect the nation's financial infrastructure. By incorporating robust threat intelligence strategies, the Treasury not only works towards maintaining economic prosperity and managing public debt effectively but also ensures resilience against evolving cyber threats, thereby sustaining a secure and competitive global economic position.

The departmental office plays a critical role within the Treasury, aligning with the department's overarching goals of maintaining economic stability and financial integrity. This division's significance lies in its 'focus on monitoring and analyzing the financial markets to prevent instability and crises. By identifying potential risks and implementing regulatory measures, it contributes to the health and stability of the U.S. and global financial systems. The department's efforts are instrumental in 'steering economic policies, managing risks, and providing expert financial analysis essential for informed decision-making at the highest levels of government'. Its work not only supports the Treasury's mission of economic prosperity but also safeguards the nation against economic vulnerabilities.

During my internship at the departmental office, within the U.S. Department of Treasury, my role was primarily focused on the domain of threat intelligence. As a Threat Intelligence Intern, I

was responsible for aiding in the identification, analysis, and mitigation of cyber threats that could potentially impact the financial stability and security of the nation. My role was pivotal in supporting the department's efforts to fortify the Treasury's digital infrastructure against emerging cyber threats.

Key Responsibilities were:

1. Threat Intelligence Gathering: I was tasked with collecting and analyzing data from various sources to identify potential cyber threats. This involved monitoring online forums, analyzing threat reports, and staying updated with the latest cybersecurity trends.
2. Analysis and Reporting: Part of my responsibility was to analyze the gathered intelligence and compile reports. These reports were aimed at providing insights into the nature of threats, their potential impact, and the likelihood of targeting the Treasury's networks.
3. Collaboration with Security Teams: I worked closely with the cybersecurity team to convey findings and suggest preventative measures. This collaboration ensured that relevant threat intelligence was integrated into the department's broader cybersecurity strategy.
4. Incident Response Support: Whenever a potential threat or breach was identified, I assisted in the incident response process. This included supporting the analysis of the incident, contributing to containment efforts, and participating in post-incident reviews to improve future responses.
5. Development of Threat Indicators: I was involved in developing and refining indicators of compromise (IoCs) that helped in the early detection of cyber threats.

Specific Projects or Tasks

1. Cyber Threat Landscape Analysis: One of my major projects involved conducting a comprehensive analysis of the current cyber threat landscape specific to the financial sector. This project aimed to identify the most pressing threats and recommend strategies to mitigate them.

2. Phishing Attack Simulation and Analysis: I participated in a simulated phishing attack project to assess the organization's vulnerability to such threats. My role involved analyzing the results of the simulation and providing recommendations for enhancing email security protocols.

3. Threat Intelligence Sharing Initiative: I was part of a team that worked on developing a framework for sharing threat intelligence with other federal agencies and partners. This initiative aimed to foster a collaborative approach to cybersecurity across the public sector.

4. Weekly Threat Intelligence Briefings: I was responsible for preparing and presenting weekly briefings to the cybersecurity team. These briefings included updates on new cyber threats, trends, and advisories from government and private sector sources.

Some key experiences and lessons learned during my internship were.

1. Cyber Threat Landscape Analysis

- Experience: Conducting an in-depth analysis of the cyber threat landscape impacting the financial sector.
- Learnings: Gained a comprehensive understanding of the sophisticated nature of cyber threats and their potential impact on national security and economic stability. Enhanced my analytical skills, especially in interpreting complex data and turning it into actionable intelligence.

2. Phishing Attack Simulation and Analysis

- Experience: Participating in a simulated phishing attack to assess organizational vulnerabilities.
- Learnings: Learned about the nuances of social engineering and its implications in cybersecurity. Developed skills in vulnerability assessment and the importance of user awareness in preventing cyber-attacks.

3. Threat Intelligence Sharing Initiative

- Experience: Working on a framework for inter-agency threat intelligence sharing.
- Learnings: Understood the significance of collaboration and information sharing in cybersecurity, gaining insights into the workings of inter-agency cooperation.

As I had lots of great experiences and learning opportunities, I also faced some challenges like.

1. Keeping Up with Rapidly Evolving Cyber Threats

- Challenge: The fast-paced evolution of cyber threats posed a challenge in maintaining up-to-date knowledge.
- Resolution: I addressed this by setting up a routine to regularly review the latest cybersecurity news and reports, attend webinars, and participate in departmental briefings.

2. Analyzing Complex Data Sets

- Challenge: Initially, interpreting vast and complex data sets for threat analysis was overwhelming.
- Resolution: I overcame this by working closely with mentors, attending training sessions, and gradually developing a systematic approach to data analysis.

3. Effective Communication of Technical Information

- Challenge: Presenting technical findings to a non-technical audience was initially challenging.
- Resolution: Improved through practice and feedback, learning to translate technical jargon into clear, understandable language.

This internship at the U.S. Department of Treasury has significantly influenced my career trajectory. My exposure to the intricacies of cybersecurity within the government sector has ignited a strong interest in pursuing a career focused on protecting national cyber infrastructure. I am now more inclined towards a career that blends cybersecurity with public service, possibly within federal agencies or government-affiliated cybersecurity firms. My time at the Department of Treasury has been transformative, contributing to both my professional and personal growth. Professionally, I have developed a set of skills, including advanced analytical abilities, technical proficiency, and improved communication skills. Personally, the experience has fostered a sense of responsibility, resilience, and adaptability. Going forward, I am equipped with not only the technical skills but also the insights into government operations, which will be invaluable in my future career pursuits. The experience has solidified my interest in a career that intersects with public service, especially in roles that focus on cybersecurity and technology policy.

I am grateful for the opportunity to have interned with the U.S. Department of Treasury. The experience has been a cornerstone in my professional development, and it has strongly motivated me to contribute meaningfully to the field of cybersecurity, especially within the context of public service. I cannot wait for my next internship journey.