Cayden Bass-hensley

4.18.2025

All In One Moving & Storage | Global Moving Services

This Paper #3 documents the completion of my full 150 hours in the cybersecurity internship at All In One Moving and Storage | Global Moving Services. Building directly on the foundation established in Papers #1 and #2, I have now moved beyond the initial onboarding phase and the early contributions that marked my first 100 hours. Paper #1 documented my introduction to the company policies, risk environment in international logistics, and the foundational observation of how cybersecurity is used to protect sensitive customer data and financial transactions. Paper #2 documented my transition to active participation, which included reviewing daily, live tracking of possible attacks, Vulnerability testing, and being more hands-on with the team. Those experiences provided me with practical context and self-confidence. The additional 50 hours documented here represent a clear continuation forward, greater independence, and a deeper integration into the security team's daily operations.

Since completing the first 100 hours, my tasks have increased to include an actual overview of key processes. I am now responsible for conducting the morning dashboard reports on our US clientele, which is a step forward compared to merely observing the U.S. traffic. My role has also grown to include proactive project work that demands deeper technical understanding. Working mostly individually, with occasional consultation with team members, I observed that the setup of custom alert thresholds was unique to logistics risks, such as securing GPS data during transit or avoiding modifications to inventory databases. I analyzed the findings and suggested changes to improve ransomware coverage in typical supply-chain businesses like

ours. With the help of a team member, we conducted independent vulnerability scans of our cloud-based warehouse management system. We then discussed our findings with the team, and some of the recommendations were spoken about in our meeting and could be adjusted before a big software update rollout. These tasks demanded that I write down my findings in a professional manner and justify my reasoning, skills that have grown noticeably since the 100-hour point.

Besides technical tasks, I also received a great experience in compliance and awareness. I was also involved in the delivery of a brief phishing-awareness training to operations personnel with access to high-value shipment information. The development of realistic scenarios using real logistics threats reinforced for me how human factors are part of the most persistent vulnerabilities in our industry.

These additional 50 hours have produced clear personal growth. I am now able to enter into meetings prepared to make observations and suggest minor improvements instead of just listening. My reading skills in complicated security scenarios, real-time troubleshooting, and reporting of findings have improved drastically. The first concepts that I learned in my courses at Old Dominion University, network defense strategies and risk assessment, have become a natural part of the routine after practicing on many occasions. The learning process is comfortable, and each challenge is progressive to develop confidence without overwhelming me.

Completing 150 hours has deepened my commitment to cybersecurity more than I expected. This internship has reaffirmed that I perform well in settings where being vigilant directly supports the success of the business. Now more than ever, I am committed to continuing my career path of pursuing a full-time position in the sphere of security operations. The foundation I have established during these 150 hours makes me eager to start the next chapter

and grateful that I can play a t role in a team that continues to keep the national and global commerce going safely.