Cybersecurity Internship: Final Reflection Paper

All In One Moving & Storage | Global Moving Services

Submitted by:

Cayden Bass-Hensley

Employer: All In One Moving & Storage | Global Moving Services

Professor Teresa Duvall

CYSE 368 / Internship

Spring 2026

April 27th, 2026

Table of Contents

Introduction

When I started looking for an internship, it was a very challenging experience. It helped me understand how important connections are in business. Fortunately, I was able to secure an internship opportunity after various outreach efforts and repeated application submissions. I was keen to find one where I could put my cybersecurity theory into practice. I secured an internship at All In One Moving & Storage, an international moving company. A logistics company posed a unique cybersecurity challenge compared to traditional IT companies because of its data-intensive nature, vast amounts of customer data, and ever-present cyber threats. This was an ideal setting to tackle both theoretical knowledge and hands-on security.

I was especially interested in how information security principles are applied to non-tech businesses. Although many cybersecurity interns work in tech firms or for the government, All In One Moving & Storage works with a large volume of personally identifiable information, transactions, and critical customer data across the nation and globally. In the Memorandum of Agreement (MOA) between All In One Moving & Storage, Old Dominion University and myself, I outlined four main objectives for my 150-hour internship: enhance my technical problem-solving and troubleshooting skills through real security-related challenges; gain practical experience in the day-to-day operations (security scanning, network monitoring, incident response, etc.); reinforce fundamental cybersecurity principles; and gain a better understanding of data protection for customer, financial and operational data. During the internship, I progressed from a passive observer to an active participant, and eventually performed independent security reviews.

Organization Overview

All In One Moving & Storage | Global Moving Services offers a wide range of logistics and relocation services, including domestic and international moving, storage, and freight solutions to various clientele. The company operates in the residential & commmercail market, and provides moving services for government and military personnel. All In One has a long history of operations in the United States and various overseas locations, with critically important digital infrastructure to support its operations.

All In One's primary lines of business include residential and commercial relocation, short- and long-term storage, international shipping, and packing and crating for valuable or sensitive goods. Much of the company's revenue comes from corporate relocation contracts, whereby, All In One is contracted to provide corporate customers with the physical and logistical aspects of workforce relocation. This model means the company is routinely handling large volumes of personally identifiable information, financial and client data, making cybersecurity a core business issue.

All In One Moving & Storage has been in business for more than 20 years, evolving from a local moving business to an major national firm. During this time, it has built out its IT infrastructure to serve its operations. These systems include cloud-based warehouse management systems, GPS-supported tracking systems, and customer portals for scheduling and tracking shipments. These tools, critical to their business operations, also represent a critical attack surface that must be monitored, defended, and manned.

From a threat perspective, logistics firms find themselves in an unfortunate position within the cybersecurity landscape. Attacks on companies in this sector are typically motivated

by the assumption that they may not have the same level of security as the typical " in the cloud" companies, and the fact that the data they manage is highly valuable, from customer credit card numbers to shipping manifests with import/export details. It quickly became clear to me in my first few weeks at the company that the threats of phishing, brute-force attacks, and other attacks were real concerns that dictated the focus of the team's efforts.

Initial Orientation and Training

The first few weeks at All In One Moving & Storage were spent on orientation and familiarising myself with the company and its security infrastructure. I was shown the company hierarchy, the position of the cybersecurity team within the IT department, and the security policies and acceptable use policies that pertained to my access and role. I was given access to security policies and procedures, which outlined how the team performed their roles.

In the early weeks, I observed a number of meetings where security matters were discussed, such as the latest threat intelligence, current patching, and compliance review activities. Although I was not yet able to participate in the technical aspects, hearing these discussions and debates was extremely helpful. I began to see how the ideas I learned in my Old Dominion University classes, network security best practices, risk management processes, policy, and compliance were being used by the security team.

The first few days of my internship with the company were quite positive. The cybersecurity team was welcoming, professional, and committed to the importance of protecting the corporate information assets of the business. What stood out to me during the orientation process was that my supervisor talked about three key principles of professionalism: detail, confidentiality, and responsibility. Similar to the Cybersecurity TRIAD, I was taught by Professor Malik Galdden and Professor Charlie Kirkpatrick. These principles were not just

something discussed as part of the policy; they were discussed in all interactions and part of the team's culture in a very real sense. I understood that I would need to live these principles myself during the internship, and I worked very hard to do so.

Management Environment

The management culture at All In One Moving & Storage was clear, open, and supportive. The cybersecurity team was part of the larger Information Technology (IT) division of the company. Within the security team, its senior security analysts managed day-to-day operations and mentored junior team members; junior analysts handled monitoring and reporting tasks. As an intern, I was placed with the junior analysts and was directly accountable to a senior analyst who was my supervisor and mentor for the duration of the internship experience.

My experience of how the team was managed can be characterised as formal mentoring. My supervisor had clear expectations at the beginning of each internship stage, gave me detailed tasks as my activities grew, and had regular meetings to review my progress, answer my questions, and give feedback. The communication culture within the team was open and professional. Everyone was accessible, and I always felt comfortable asking questions and voicing a concern. This greatly sped up my professional development.

The management structure was evidence of a commitment to considering cybersecurity as a strategic rather than an operational support function. The CEO was included in the business planning discussions at the highest levels of the business, and security objectives were considered when evaluating changes to processes, relationships with clients, and technology purchases. This high-level support for a culture of security permeated throughout the entire organisation and provided an appreciation for the value of the security team's work.

At the operational level, the management hierarchy at All In One Moving & Storage was well structured to accommodate both the needs of its multinational logistics business and my learning journey as an aspirational cybersecurity professional. I had a supportive, approachable supervisor who empowered me as my skills and knowledge increased. It was undoubtedly part of the management strategy to progressively increase my involvement - from observer to active participant. This demonstrated a working perspective, one that took the development of the interns seriously, rather than simply employing them as extra hands.

Major Work Duties, Assignments, and Projects

My duties as an intern grew considerably over the three stages of my 150 hours. My early days of observation and learning evolved into more active involvement in the work of the security team. The subsections that follow outline my primary responsibilities, tasks, and projects that progressed throughout the internship.

Security Log Reviews and Monitoring

One of the first tasks I worked on was helping with the periodic monitoring of security logs. This included monitoring and reviewing network traffic and events from the company's locations, reviewing event logs for unusual patterns, and escalating potential threats for further investigation and response. This role is vital for the company, as timely detection and response to threats is key to avoiding data breaches and the associated business impact. One remarkable instance came during an afternoon shift, where we noticed a dramatic increase in unsuccessful login attempts from an unknown IP address associated with one of our shipping-tracking software. This incident involved collaborating with the team to investigate the activity, which we identified as a brute-force attack, and quickly blocked the offending IP address. Being part of the

entire incident response (detection, analysis, and mitigation) was a very powerful learning moment for me. It further highlighted how important ongoing security monitoring is.

In the last few weeks of my internship, my involvement in this process grew. I moved from assisting with log reviews to creating and presenting daily reports with junior staff for the U.S. via the dashboard. This required strong critical thinking and judgement to identify the issues that needed attention from the team before the start of the day.

Vulnerability Scanning and Assessment

In the second and third stages of my internship, as my responsibilities grew, I worked on vulnerability scans of critical company resources such as the internal inventory management software and the cloud-based warehouse management system. Alongside a senior analyst, we used the scanner Nessus to conduct thorough scans and then delved into the reports to pinpoint issues. This required not only interpreting the reports but also using judgment to isolate issues that were a real threat to operations from those that were less relevant to the company's environment.

This activity is critical to the company as vulnerabilities in the digital infrastructure of a logistics company, particularly in a global environment with systems at remote sites, can be used to facilitate attacks and/or unauthorised access to data with potentially severe financial and reputational impacts. By proactively identifying weaknesses before adversaries can exploit them, the security team plays a direct and measurable role in protecting business continuity.

I was given more complex tasks during the last 50 hours (out of 150 hours) of my internship. I tested the security of the corporate Warehouse Management System (which is hosted in the cloud), wrote a small report, and provided security recommendations to the team.

Firewall Testing

I was given some training on designing the company's firewall and witnessed testing the rules that controlled the flow of traffic between the national and offshore partners. This provided me with some exposure to overseeing, managing, and testing access control for a large multi-site company, which was new to me. This required some technical expertise and a delicate balance to ensure this did not impact the business.

Custom Alert Threshold Configuration

In the last few weeks,s I had the chance to take part in the configuration of custom thresholds for alerts for the logistics sector. I assisted the team as needed to set up alerts for such threats as GPS spoofing in transit, failed login attempts, and spoofing of customer and inventory data. These threats are vital for enterprise security.

The junior team, along with the help of the senior analyst,e reviewed the alert system and provided recommendations for alerting for threats like attacks on the supply chain. We then presented the findings in a meeting and documented our findings, which can be used in the update. This project was a chance to apply my technical, judgment, and communication skills at work.

Phishing Awareness Training

Another project I enjoyed working on was a phishing presentation for our operations staff. They are frequently the targets of social engineering schemes because they have access to shipping and customer data. We helped to develop industry-specific phishing scenarios and presented the material in a non-technical way. This helped me to understand the human element of cybersecurity, and also explained technical concepts as well.

Cybersecurity Skills and Knowledge Applied

Pre-Internship Skills

Before my internship with All In One Moving & Storage, I had been introduced to many of the basic cybersecurity concepts through my studies at Old Dominion University. I came to the internship with basic knowledge of fundamental network security concepts, a conceptual understanding of cryptography and encryption, basic knowledge of risk assessment techniques, and awareness of various types of cyber threats such as phishing, malware, and ransomware. I was also comfortable working within Linux-based environments and had been introduced to tools such as Wireshark and basic network scanning utilities through academic laboratory exercises.

This was a good foundation for basic theoretical knowledge, but I was well aware before starting the internship that there was a disconnect between theory and practice, especially since this was my first internship opportunity. I knew of a cloud management system but had never worked with one. I understood vulnerability assessment approaches, but had no experience with enterprise-level assessment tools like Nessus. I knew about firewalls, but had experience working with them in a real-world cybersecurity environment. The internship served, in part, as an opportunity to gain real-world experience to fill in these gaps.

Skills Developed on the Job

The internship was successful in addressing these skill gaps and taught me skills I didn't expect to learn. Through my experience using the company's cloud management system, I was able to practice real-time operational-level security monitoring for an extended period of time. I learned to navigate network security dashboards, event logs for monitoring, and to identify patterns of unusual or suspicious activity and escalate as per team procedures. This provided me

with real-world experience, which translated my basic knowledge of security monitoring from the academic environment to the industry.

I experimented with vulnerability scanning software like Nessus to perform regular scans and to understand technical reports. I also learned to prioritise the results of the scan based on criticality and impact, a skill that extends beyond technically scanning a network. I also became adept at testing the effectiveness of firewalls and developing custom alert rules tailored to specific risk classes.

I also gained significant professional skills that I didn't expect to be a primary focus of the internship. I had to communicate technical concepts and information clearly to colleagues in security reports, technical presentations, and awareness training. These skills are just as crucial to a cybersecurity practitioner's success as any technical skill, and I am thankful that the internship provided a platform to use them in practice.

Change in Understanding

My professional experience at All In One has also changed my understanding of cybersecurity as a field and a profession. Before the internship, I was inclined to view security from a technical perspective - as a series of tools, configurations, and policies that hinder an outsider's ability to gain access. Having spent 150 hours immersed in a multinational logistics company, I now see cybersecurity as much more than this: an ongoing discipline of the organisation that involves technology, risk, policy, human behaviour, and business simultaneously.

I found that the human factor - awareness, compliance, and culture - is one of the most important and enduring factors in an organization's security posture. Even the best-designed

technology controls can be defeated with a single phishing email to an unwary employee. This will guide and shape my career in security.

ODU Curriculum and Internship Preparation

Connections Between Academic and Professional Experience

The knowledge I gained at Old Dominion University was extremely useful throughout my internship. I was able to apply what I learned in class to the real world. Lessons in network security, fundamentals of cybersecurity, and risk management provided the theoretical basis for me to rapidly comprehend the tools and processes used by the security team. Most importantly learned how to work with team members in a professional setting. On the first day of orientation, I was able to grasp conversations regarding threat intelligence and access controls. This enabled me to engage in discussions and ask valuable questions.

The most direct and consistent academic connections I experienced were in the areas of network defense, vulnerability assessment, and risk-based decision making. Theoretical concepts that I had learned about, from Professors Kirkpatrick and Gladden at ODU, such as the way vulnerabilities are classified by the NIST framework, and the concept of network security, were evident in my work. I understood these concepts on a new level, which transcended theoretical learning.

Experiences That Reinforced School Learning

Several specific internship experiences reinforced and validated what I had learned during my academic program at ODU. Performing vulnerability scans and reviewing the scan reports were very similar to the vulnerability assessment techniques I had learned, and the real-world experience validated the knowledge and skills I had gained in this field. Conversations regarding network traffic monitoring, detection, and incident response mirrored

the topics covered in my network security classes. The discussions of documentation, reporting, and the ability to effectively communicate security issues also reinforced the analytical and writing skills on which I had been focusing during my academic studies.

New Concepts and Skills Not Encountered in School

On the other hand, this experience also brought me into contact with several areas not extensively covered in my ODU classes. The logistics-specific nature of the security problems at All In One, the need to protect the integrity of GPS data while in transit, to comply with multiple jurisdictions' data privacy and protection laws, and to consider the security implications of the global supply chain's architecture, were not heavily featured in my academic studies. These are niche issues, but they are hugely important to the logistics industry, and I was able to gain a sense of how cybersecurity challenges are unique to different industries.

Large-scale operations, the rationale behind setting custom alert thresholds, and the coordination of cybersecurity processes with globally dispersed teams were other aspects of cybersecurity work that I had not previously encountered in the classroom. Most importantly, creating and delivering phishing education to a non-technical audience was a new and exciting experience. Phishing always excited me as I learned about it in the classroom, so presenting that project with the team was the highlight of my internship experience. Although social engineering was discussed in my coursework, it did not prepare me to put those lessons into a teaching format for the daily workforce. This was an important addition to my work experience.

Learning Outcomes: Fulfillment of Internship Objectives

Objective One: Technical Troubleshooting Skills

The first of my learning objectives was to acquire technical troubleshooting skills. This learning goal was completely met in all three parts of my internship. As soon as I started helping

with daily security log reviews and monitoring, I was exposed to numerous opportunities to identify anomalies, locate the source of various suspicious network events, and work out possible explanations before escalating the results. One of the clearest examples came when the team detected an unusual spike in failed login attempts tied to an unknown IP address. Through the analysis process, and with the help of senior analysts, we were able to verify the brute-force attack and how it was addressed. As my responsibilities grew, monitoring vulnerability scans, analysing results, and performing configuration reviews - all required well-organised and systematic troubleshooting. After my 150 hours of work, my analytical thinking skills to come to a logical conclusion on a technical security issue were vastly improved from the beginning.

Objective Two: Hands-On IT and Cybersecurity Experience

My second learning objective was to gain substantive hands-on IT and cybersecurity experience. My previous experience in the field had consisted primarily of classroom knowledge and lab-based experimentation. This goal was well met. During the 150 hours I spent there, I went from being an observer to contributing to the day-to-day work of security practitioners. I used the company's system to track network traffic, used the vulnerability scanner Nessus to scan production systems, helped to test the company's firewalls, helped to validate the company's scheduled update, created custom alert thresholds, and co-presented a phishing awareness training program. These were all real tasks and activities that provided valuable IT and cybersecurity experience; not simulations, but actual work with actual impacts to the business. This experience was much richer and more varied than I expected, and it will provide a valuable baseline for my future career.

Objective Three: Basic Cybersecurity Principles

The third learning goal was to gain a better understanding of basic cybersecurity principles by observing how they were applied. This objective was met throughout the learning experience. Principles such as network security, firewall testing, vulnerability scans, network defense, and threat detection were all in use by the security team regularly. Using these principles in a live setting added more meaning to the concepts. For instance, while I learned about brute-force attacks in class, observing the team identify, assess, and block a real brute-force attack had a deeper impact. After 150 hours, these foundational principles evolved from abstract knowledge into an intuitive way of thinking about security challenges.

Objective Four: Understanding Data Protection and Security

My fourth objective was to learn about data protection and security, how an organisation identifies, classifies, and protects its sensitive data. This learning objective played out in a way that was more comprehensive and subtle than I expected. At All In One Moving & Storage, data protection is not a unified system or a set of rules, but a company-wide process that permeates the entire organisation. I learned how certain information, such as customers' personally identifiable information (PII), financial transactions, and even manifests on the ships transporting storage around the world, all have different security requirements and how the security team ensures those requirements are upheld through cloud & data platforms. My work in setting alerts to quickly identify when someone is trying to alter the database of inventory items and training employees who handle high-value shipment data on how to avoid phishing scams all helped achieve this goal. As a result of my internship, I understand why protecting data is the primary focus of any cybersecurity program, and I have helped achieve that goal.

Motivating and Exciting Aspects of the Internship

The most exciting and motivating aspects of my 150-hour internship with All In One Moving & Storage were the times when the work was tangible, real, and had a profound impact in ways that classroom exercises cannot duplicate, most importantly, the presentation of the Phishing Exercise was most exciting in this experience. Outside of this experience, my continuous professional development was another motivating factor. The deliberate journey from understanding to participation, and ultimately learning and understanding vulnerability assessments and building phishing training resources, gave me a strong sense of pride and ownership of my work. Knowing that my reports were being reviewed for software updates and that the training materials the junior team and I helped create were equipping operations staff to defend against real threats gave me a profound sense of purpose. Moreover, the nature of the company's operations ensured that the challenges were never dull as we continually addressed security concerns within our systems. This kept my learning curve alive and provided opportunities to learn and grow.

Discouraging Aspects of the Internship

Even though my experience working for All In One Moving & Storage was overwhelmingly positive, there were elements of the internship that were disappointing or professionally frustrating, and it's important to acknowledge these in this report.

The most significant source of frustration during the internship was the pace of the initial orientation phase. During the first few weeks, my work was mostly observational - reading policy documents, attending meetings, but not in a specific technical capacity, and getting to know the department. I knew intellectually that this was a normal and professional way to

integrate a new team member, and my supervisor made it clear that this was a period of time and one that would pass. I was, however, keen to be involved, and there were moments in the early weeks where I felt under-challenged and frustrated at not being more involved. As such, patience and vigilance during this time of onboarding, and acceptance of the benefits of the knowledge being acquired, were a valuable lesson in themselves.

I struggled with imposter syndrome a lot. Being that I had no prior hands-on experience, I constantly faced thoughts of not being smart enough to understand all the technical things in the cyberworld on this scale. I also found it occasionally frustrating to use certain systems in use at outlying warehouse sites or partner sites overseas, which were not the latest technology, and the security challenges they presented could sometimes not be easily overcome.

Finally, at times I was overwhelmed by the wide range of threats faced by the company, and knowing that, being in the IT/Cyber team, we were responsible for monitoring it... The realm of security challenges, when seen all together, could be overwhelming, and I had to remind myself that the team did not strive to eliminate all risk but rather to manage it effectively and on an ongoing basis.

Challenging Aspects of the Internship

The most difficult parts of my internship were those that challenged me to do more (much more) than I currently knew and was able to do, and to learn new skills within the constraints of the professional environment. These challenges were ultimately the most valuable experiences of the internship, precisely because they demanded more of me than I could have provided at the outset.

The most technically challenging activity I completed was the vulnerability assessment on the cloud-based warehouse management system, during the last 50 hours. Jointly with the junior team, we were required to independently execute the scan, analyse the results, prioritise the findings from a business perspective, and prepare a report for review and action by other team members and managers. This meant that we had to simultaneously apply technical skills, analytical reasoning, and professional writing skills - all while not having a senior analyst looking over my shoulder to be guided. That independence was both the most challenging and the most professionally meaningful aspect of the entire internship.

Delivering the phishing training was also challenging, but in a way that I hadn't expected. I was well-prepared with the technical aspects of the presentation. But when delivering the content to a live audience of operations staff, many of whom were cynical about or bored with technology, I had to tailor my delivery style, answer questions I had not anticipated, and keep the audience engaged. This helped to build my self-confidence as a professional communicator in a way that I had not experienced with academic presentations.

Perhaps the greatest challenge throughout the internship was simply getting used to the professional working environment. Universities offer flexibility not found in the workplace. Learning to consistently meet workplace expectations, communication, professional documentation, and the flow of an actual work week took time and consideration. This transition isn't uncommon, but I feel that it is important to acknowledge it for the sake of future interns who may also experience it.

Recommendations for Future Interns

Based on my full 150-hour experience at All In One Moving & Storage | Global Moving Services, I offer the following recommendations to students who may be considering this internship in future semesters.

Understand the basics of network security before starting the internship. The organization will provide orientation and training on their tools, but if you come with a basic understanding of how these tools are used to collect security data and how security analysts use dashboards to spot anomalies, you will feel more comfortable and able to contribute sooner in the transition from observation to contributing. There are free academic educational resources and lab setups that can aid in this preparation.

Spend time familiarising yourself with vulnerability scanning approaches and tools. Being able to perform scans, interpret the results, and present findings in a meaningful way is a fundamental skill of the junior analyst role that interns will be expected to take up over the course of their internship. Read the free, publicly available documentation on the Cybersecurity Frameworks, such as NIST, and familiarize yourself with these things.

Take time to be an observant intern. The initial period of the internship may seem boring and unwarranted to students keen to get their hands on some technical work, but it is important. The knowledge you gain of the context in which you are working by observing the team, reading policy documents, and attending meetings will serve you well during the rest of the internship. Do not passively wait for activities to come to you; ask questions, take notes, and use every meeting as a learning opportunity.

Develop communication and writing skills before the internship. Clear, coherent, well-organized security reports and the ability to communicate effectively to both technical and non-technical people are as critical to success in this field as any technical ability. Students who can clearly communicate and write will stand out and be more effective. Work to improve this skill in your academic work and use each writing assignment to improve your skills.

Finally, read up on cybersecurity issues relevant to the industry that you may be doing your cyber work in. Knowing why these companies are targeted - the nature of the data they handle, and how attacks can affect them will be invaluable in understanding all of the projects you will see during your internship. Reading threat intelligence reports focused on your industry and studying key cybersecurity incidents will get you ahead of the game in a way that will be apparent to your team.

Conclusion

Main Takeaways from the Internship

The 150-hour internship with All In One Moving & Storage | Global Moving Services is one of the most important professional experiences in my career. The biggest takeaway was a greater understanding of the challenges, risks, and human aspects of cybersecurity. Cybersecurity is not just an academic exercise, but a dynamic and evolving field that requires constant vigilance, critical thinking, and good communication to keep people, systems, and data safe.

I also gained a better understanding of the nature of cybersecurity jobs. It involves discipline, analysis, communication, adaptability, and working in risky environments. These skills have been developed through increasingly challenging practical experience, and I believe I am now much better equipped for a career in the work industry.

Influence on Remaining College Experience at ODU

My time at All In One Moving & Storage will have a significant impact on the remainder of my academic career at Old Dominion University. I will now make more informed academic decisions, given my understanding of which skills are in demand in industry. I will prioritise classes in cloud security and compliance and regulatory requirements, and advanced network monitoring, areas in which I saw a significant disconnect between academic education and industry expectations.

Influence on Future Professional Path

Looking to the future, my internship has both affirmed and strengthened my intention to work in cybersecurity operations. My experience of working as part of a security team, contributing to the ongoing work of detecting threats and managing vulnerabilities, and witnessing firsthand how security operations support business processes has confirmed to me that this is the career I am committed to ppursuing In particular, I am especially interested in roles in Security Operations where the constant monitoring, incident response, analysis and action I learned at All In One is the primary professional practice.

The skills and insights I have developed in these 150 hours, in technology, communication, and awareness of my own role in an organization, have served me well as I embark on the next phase of my training. I am thankful to have been included in a team that takes its responsibilities seriously, that invested in my development and growth as a member of the team, and that has allowed me to become skilled and confident in a career for which I am passionate. I am eager to apply what I have learned from this internship to all my future professional experiences.