

CYSE 368 Internship Final Paper

Shauntell Gavino-Collins

Cavalier Logistics

Mr. Collins, Network Consultant

CYSE 368 Internship Fall 2025

December 01, 2025

Table of Contents

- 1. Introduction**
- 2. Management Environment**
- 3. Work Duties & Assignments**
- 4. Use of Cybersecurity Skills & Knowledge**
- 5. ODU Curriculum Connection**
- 6. Learning Outcomes Reflection**
- 7. Motivating Aspects**
- 8. Discouraging Aspects**
- 9. Challenging Aspects**
- 10. Recommendations for Future Interns**
- 11. Conclusion**

1. Introduction

When I started looking for internships, Cavalier Logistics stood out because they had an incredible flexible schedule and let interns work on real network security issues instead of simply shadowing people all day. The company is based in Sterling, Virginia, and they handle transportation and supply chain management, air freight, ocean freight, warehousing, and distribution. With offices across multiple states, they rely heavily on their network infrastructure to keep everything running smoothly between locations. I wanted a hands-on experience in a real business environment, and this seemed like the perfect opportunity.

Cavalier Logistics operates in a highly competitive industry where timing is everything. A delayed shipment or compromised client data could mean losing contracts worth millions of dollars. This reality made the cybersecurity work feel urgent and meaningful from day one. Understanding the stakes helped me appreciate why every firewall rule and access control decision mattered so much.

My long-term goal is to work in forensic accounting and cybercrime prevention, so I wanted to understand how companies protect their digital infrastructure and sensitive client data. This internship let me see both the technical side of cybersecurity and how it fits into actual business operations in the logistics industry. The logistics sector faces unique cybersecurity challenges that I hadn't fully appreciated before. Unlike financial institutions or healthcare providers, or other industries, logistics companies must maintain security while coordinating with countless external partners, freight carriers, customs brokers, warehouse operators, and international shipping lines. Each external connection represents a potential vulnerability, which meant I got to see how security professionals balance openness for business efficiency with protection against threats.

Before starting, I set three main goals. First, I wanted to get comfortable working with enterprise-level networking equipment and cloud-based management platforms, specifically Cisco Meraki access points, routers, switches, and firewalls. Second, I wanted to understand how network security policies get implemented across multiple locations, including things like network segmentation, VPNs, and traffic monitoring. Third, I hoped to improve my analytical and communication skills by working directly with my supervisor, Mr. Collins, to learn how cybersecurity principles translate into daily decisions.

My first day at Cavalier Logistics included the usual orientation activities such as safety briefings, data security training, and tours of the network operations area. My initial impression was quite positive also due to the company having a professional atmosphere, but people were also collaborative and willing to teach. What stood out most was that cybersecurity wasn't treated like some background IT department; it was clearly important to every part of the business. During the orientation, the HR representative explicitly mentioned that network

security incidents had cost the company significant revenue in previous years, which explained why security was taken so seriously across all departments. That made me realize I was joining an organization that had learned hard lessons about the business impact of cybersecurity failures.

2. Management Environment

I worked directly under Mr. Collins, the company's Network Consultant, who served as both my supervisor and mentor. His management style was hands-on but also gave me room to learn independently. He didn't just tell me what to do either, he encouraged me to observe, ask questions, and actually understand the systems we were working with. We had weekly meetings to review what I was working on, discuss any network issues that came up, and make sure my projects aligned with what the company needed.

What impressed me most about Mr. Collins's approach was his emphasis on understanding the "why" behind every technical decision. When we reviewed firewall configurations, he wouldn't just show me the rules, he would explain the business logic driving each policy. For example, when discussing why certain IP ranges were blocked, he'd trace it back to previous security incidents or compliance requirements from specific clients. This contextual teaching method helped me develop intuition about security architecture rather than just memorizing procedures. He also encourages me to question existing configurations and propose alternatives, which built my confidence in technical decision-making even as an intern.

Mr. Collins also modeled professional growth in meaningful ways. He regularly attended industry conferences and vendor training sessions, often sharing insights from these experiences during our meetings. He subscribed to multiple cybersecurity newsletters and threat intelligence feeds, demonstrating that staying current isn't optional in this field. Watching him dedicate time to continuous learning, despite his busy schedule, reinforced that cybersecurity professionals must commit to lifelong education. He also connected me with other IT professionals in the company, creating networking opportunities that broadened my understanding of how different specializations collaborate.

The management structure at Cavalier includes specialized teams across IT, logistics coordination, accounting, and operations. The network security division plays a central role because if the network goes down, pretty much everything else stops working. I got to see how different departments communicated with each other, especially when network changes affected customer-facing systems or warehouse operations. It showed me that cybersecurity can't exist in a vacuum, it has to support business goals, not just protect systems for the sake of protection.

One particularly illuminating experience involved sitting in on a cross-departmental meeting about implementing multi-factor authentication for warehouse management systems. The IT team advocated for strict security controls, while operations managers worried about slowing down time-sensitive shipping processes. Watching Mr. Collins navigate these competing

priorities taught me valuable lessons about stakeholder management. He presented data on authentication times, proposed phased implementation, and demonstrated how security could actually improve efficiency by reducing password reset calls. This approach helped me understand that technical expertise alone isn't enough, successful cybersecurity professionals must also be skilled negotiators who can translate security needs into language that resonates with different audiences.

The management culture emphasized accountability and fixing problems before they became bigger issues. Every configuration change, security update, or access modification had to be documented and reviewed. This reminded me of the chain of custody principles we learned in class, maintaining the integrity of data and keeping records is crucial for both security and compliance. Mr. Collins also emphasized ethical responsibility, which reinforced what I'd learned about how even small shortcuts in documentation could create long-term vulnerabilities.

I believe the management environment worked really well. The balance between supervision and independence gave me freedom to apply what I'd learned in class while still having professional guidance. I learned that good leadership in cybersecurity isn't about micromanaging, it's about creating an environment where people feel comfortable asking questions and taking their work seriously.

3. Work Duties & Assignments

As a Network Security Intern, I did a mix of hands-on configuration work and observation of larger enterprise systems. My main responsibilities included helping deploy, monitor, and document Cisco Meraki MR-56 Access Points, which provided cloud-managed wireless networking across multiple Cavalier facilities. I learned to use the Meraki dashboard to configure SSIDs set up network segmentation for staff and guest users and monitor performance metrics across all seven states where Cavalier operates. What impressed me most was how scalable the system was and how we could add new sites remotely without taking anything offline.

Working with the Meraki system introduced me to the practical side of wireless security that textbooks can't fully capture. I learned about the delicate balance between signal strength and security, too powerful and you're broadcasting your network beyond your physical premises, creating opportunities for parking lot attacks; too weak and legitimate users experience connectivity issues. Mr. Collins showed me how to use heat mapping tools to optimize access point placement, ensuring adequate coverage while minimizing signal bleeding into public areas. I also learned to configure rogue access point detection, which automatically alerts administrators when unauthorized wireless devices appear on the network. During one incident, this system detected an employee who had connected a personal router to bypass network restrictions, a seemingly innocent action that could have created a significant security vulnerability.

One of the major projects involved working with Cisco FPR1010-NFGW-K9 Next Generation Firewalls. These devices are critical for maintaining secure connections and protecting data as it moves between networks. I worked with Mr. Collins to review firewall configurations, analyze traffic patterns, and verify that access control lists (ACLs) were blocking unauthorized activity. This gave me real insight into how modern firewalls use deep packet inspection and advanced threat detection to defend against breaches.

The firewall work particularly fascinated me because it revealed the cat and mouse nature of cybersecurity. During one session, Mr. Collins showed me the logs where the firewall had blocked hundreds of automated attacks originating from international IP addresses. These weren't sophisticated attacks, just automated scripts scanning for common vulnerabilities, but their volume was staggering. I also learned about false positives and the challenges of tuning firewall rules to minimize traffic disruption. Finding that balance requires understanding both network behavior patterns and business operations.

I also spent time working with Cisco routers and switches. Mr. Collins showed me how to configure VLANs to separate VoIP systems from data networks, which ensures both web applications and phone systems work properly. I got to see how properly configured access lists and routing policies prevent broadcast storms and keep the network reliable. This helped me connect the theoretical networking concepts from class to actual enterprise configurations.

Another learning experience was working with VeloCloud SD-WAN devices, which optimize wide-area network performance and provide redundancy across multiple ISP circuits. These systems help ensure that if one internet connection goes down, the network automatically switches to a backup. I shadowed Mr. Collins during ISP circuit installations and saw how coordination with vendors and troubleshooting protocols kept business running during outages. These experiences showed me that technical skill is important, but so is communication, you have to be able to explain issues clearly to service providers and other stakeholders.

One particularly memorable project involved documenting the company's disaster recovery procedures. Mr. Collins assigned me to review existing documentation and identify gaps or outdated information. This task initially seemed tedious, but it taught me how crucial documentation is for business continuity. I discovered procedures referencing equipment that had been replaced years ago and contact information for vendors who no longer provided services. Updating this documentation meant speaking with various team members, verifying current procedures, and creating clear step-by-step guides. This project demonstrated that cybersecurity extends beyond technical implementation to include organizational preparedness, ensuring that when incidents occur, teams can respond quickly and effectively.

Looking back, these projects showed me how network security functions as a living system. Every device, from a firewall to a wireless access point, is a layer in the organization's defense

strategy. Getting to participate in this environment gave me a front-row seat to see how all these layers work together to protect the confidentiality, integrity, and availability of business operations.

4. Use of Cybersecurity Skills and Knowledge

I came into the internship with a decent foundation from my ODU classes, I understood the basics of encryption, authentication, access control, and network segmentation. Working with these concepts in a real production environment was completely different from taking exams about them. Everything was more connected and complicated than I expected. Working with the Cisco Meraki MR-56 Access Points was a good example. In some of my classes, I learned about how user segmentation and access policies as separate concepts. At Cavalier, I saw how they directly affected both network speed and security at the same time. The Meraki cloud dashboard was honestly fascinating; Mr. Collins could manage wireless access across all seven states from one screen. It made me realize how much cloud-based tools have changed IT work, especially for companies with multiple locations.

The practical application of encryption protocols was particularly eye-opening. From my classes, we discussed WPA3 and certificate-based authentication theoretically. At Cavalier, I helped implement these protocols and immediately encountered real-world complications. For instance, legacy devices used by warehouse scanners couldn't support the latest encryption standards, forcing us to maintain separate network segments with older protocols. This created a security trade-off that required careful risk assessment, do we upgrade expensive equipment prematurely, or do we accept calculated risk while implementing compensating controls? These decisions involved cost-benefit analyses that classroom scenarios rarely capture.

Working with the Next Generation Firewalls really deepened my understanding of enterprise-level protection. Firewall rules aren't just abstract configurations; they reflect the company's actual operational priorities and balance usability with security. I also learned to read logs, analyze blocked traffic, and identify suspicious activity patterns. Configuring VLANs and access lists on routers and switches also helped me see how network segmentation can minimize the spread of potential breaches.

One of the most interesting lessons came from watching how VoIP systems and web applications are integrated securely. Seeing Mr. Collins configure VLANs to support VoIP showed me that cybersecurity goes beyond just protecting devices, it ensures reliable communication for the entire organization. I also got familiar with auditing configurations, documenting changes, and reviewing compliance logs. The on-the-job learning expanded my skill set way beyond the classroom. I got better at troubleshooting connectivity issues, using monitoring tools to interpret system alerts, and recognizing when automation can improve reliability. I also learned that human factors play a huge role in cybersecurity, even the most advanced hardware can fail if

users ignore best practices or skip documentation. This changed how I think about the field: cybersecurity isn't just a technical discipline, it's an ongoing process of staying on top of threats that are continuously adapting.

5. ODU Curriculum Connection

My education at ODU gave me a strong foundation that translated well into my internship at Cavalier Logistics. Courses like CYSE 200T Cybersecurity, IT 205 Introduction to Object-Oriented Programming, IT 201 Introduction to Information Systems, CRJS 310 Cybercriminology: Foundations, and CYSE 406 Cyber Law, gave me the framework to understand what I was seeing and contributing to. Theories about layered defense, redundancy, and threat modeling became tangible when I worked with the company's actual infrastructure. I could see how the discussions in one of my classes about the CIA Triad, which revolved around confidentiality, integrity, and availability, played out through access control configurations, firewall policies, and backup systems. Other ways that my classes helped me was not only preparing me with awareness but gave me information regarding VPN setups, encryption protocols, authentication, lessons on ethical hacking, and vulnerability assessment.

However, the internship also exposed areas where academic preparation meets real-world constraints. While ODU taught me to design and analyze secure networks conceptually, Cavalier Logistics taught me how to implement them practically within the limits of cost, business needs, and scalability. In the classroom, cybersecurity is often isolated from other business operations, but this internship showed me how deeply interconnected security is with finance, logistics, and human resources. Network downtime doesn't just affect data, it disrupts shipments, delays transactions, and impacts the company's reputation.

Through this experience, I also discovered new areas I want to learn more about. I developed a stronger interest in cyber risk auditing and compliance management, which align with my future goals in forensic accounting. The internship made it clear that the most effective cybersecurity professionals understand both the technical infrastructure and the organizational ecosystem that depends on it. ODU's interdisciplinary approach prepared me well for this but the internship gave me the perspective and confidence to actually apply it.

6. Learning Outcomes Reflection

The first goal I set before starting was to gain hands-on experience with enterprise-grade networking tools and systems. I definitely achieved this through daily work with Cisco Meraki MR-56 access points, next-generation firewalls, routers, and switches. Each week brought new technical challenges, from configuring VLANs for traffic segmentation to checking VPN tunnel stability between Cavalier's regional branches. By shadowing Mr. Collins during configuration reviews and change-control meetings, I learned not just how to do things, but why they're done that way. For example, firewall rules weren't just lines of code, they reflected carefully thought-

out business policies that balanced operational access with risk tolerance. Being able to connect these technical decisions to organizational strategy confirmed that I was developing both technical competence and strategic awareness.

My second goal was to understand how cybersecurity supports business continuity across different locations. Cavalier Logistics was perfect for this because their operations span multiple time zones, and connectivity problems could, again, delay shipments and hurt client relationships. I saw firsthand how redundancy, through SD-WAN failover paths and cloud-managed wireless systems ensured that no single outage could shut down communication. During one incident when an ISP circuit briefly failed, I watched Mr. Collins redirect traffic through a backup link within minutes. Seeing that rapid response reinforced that cybersecurity is as much about resilience and recovery as it is about prevention.

The third goal was to develop professional communication and problem-solving skills, which I definitely accomplished. Early on, I sometimes hesitated to ask questions during technical discussions because I didn't want to interrupt. Mr. Collins encouraged me to speak up, reminding me that asking questions is how you actually learn. Over time, I got more comfortable articulating technical observations clearly and concisely, and I learned to translate complex networking issues into language that non-technical staff could understand. That ability to communicate risk and recommend solutions across departments turned out to be one of the most valuable skills I gained.

An unexpected but equally important outcomes was developing a stronger sense of ethical responsibility. Handling access credentials, monitoring user activity, and viewing internal traffic data all required discretion and professionalism. The internship reinforced that cybersecurity practitioners are responsible for protecting trust, every log entry or configuration command has ethical implications. Taking this responsibility seriously deepened my respect for the field and confirmed that ethics isn't just an abstract course topic, it's a daily practice that defines your credibility.

7. Motivating or Exciting Aspects

The best part of the internship was knowing my work actually mattered. When I helped configure something that protected data from moving between warehouses, or when a firewall rule, I worked on blocked a potential threat, it felt real. It wasn't just practice anymore, it was protecting actual company operations. I'll admit, every successful deployment felt pretty satisfying because there is something motivating about seeing your preparation pay off, especially when you're working with a team and know that clients are depending on this on this stuff to work correctly.

Working with cutting-edge technology in a real business setting is also exciting. Cisco's Meraki dashboard fascinated me because it showed how cloud computing can change network

administration. Through one interface, our team could monitor wireless devices across seven states, review bandwidth usage, and push firmware updates remotely. I gained new appreciation for how scalable cloud-based systems are and how they let small IT teams manage huge infrastructure efficiently. This experience helped me see the future of enterprise networking, where automation and visibility reduce human error and speed up response times.

Another motivating factor was the mentorship culture. Mr. Collins consistently connected technical lessons to bigger professional themes. For example, after trouble shooting a VLAN misconfiguration one day, he explained how similar issues could create serious vulnerabilities if left undocumented. These conversations transformed routine tasks into real learning moments and showed me how experienced professionals think strategically. They also taught me that mastering cybersecurity involves constant curiosity, willingness to adapt, and learning no matter what is new in the field.

The internship renewed my enthusiasm for combining cybersecurity with forensic accounting. I started imagining how similar investigative approaches could be applied to financial systems to detect fraud or anomalies. That realization got me genuinely excited about designing a career that combines technology with financial integrity.

8. Discouraging Aspects

The internship was great overall, but it definitely had some frustrating parts. The biggest one was not having access to the more critical production systems. I get why, they can't let interns accidentally break important stuff, but it meant I spent a lot of time watching instead of doing it. During maintenance windows, I basically sat on the sidelines. At first, it was frustrating because I wanted to experience it hands-on and not just observing. Eventually I realized I was still learning a lot by watching Mr. Collins work through problems, and I started taking better notes so I could try things later in a test environment. But yeah, I wish I could've done more configuration work.

Another thing that took getting used to was the invisible nature of success in cybersecurity. In many cases, a day with no incidents just meant systems were working correctly, but that normalcy could feel anticlimactic. Unlike other fields where you can see your progress, network security often rewards silence and stability. It took time to accept that prevention, not reaction, is the real measure of success. Once I shifted my perspective, I found, in a way, a sense of accomplishment in maintaining security and ensuring calm rather than waiting for crises to be resolved.

I also occasionally felt the strain of communication gaps between departments. When technical jargon clashed with logistics terminology, misunderstandings could slow down decision-making. Watching Mr. Collins navigate those situations taught me the importance of empathy and clarity. Security professionals must translate risks into operational language that makes sense to non-

technical people. Although these communication challenges were sometimes frustrating, they provided important lessons in diplomacy and patience, qualities that will help me in any collaborative environment.

9. Challenging Aspects

The most demanding part of the internship was learning to balance security, performance, and usability. Every configuration change involves trade-offs. Strengthening encryption could slow things down; tightening access controls might make things less convenient for remote users. Understanding how to strike the right balance requires both technical knowledge and understanding organizational priorities. Through testing and feedback, I learned that effective security design is as much an art as a science, it must protect without making it impossible to get work done.

Another major challenge was interpreting network anomalies in real time. When monitoring the Meraki dashboard or firewall logs, spikes in traffic or unusual IP connections could signal potential intrusions, but they required contact to understand. Early on, I found the volume of data overwhelming, but with guidance, I learned to filter alerts, establish baselines, and use data visualization to spot meaningful patterns. This process improved my analytical discipline and reinforced the importance of staying calm and evidence-based under pressure.

Time management also turned out to be harder than expected. Balancing multiple small projects, documentation updates, configuration checks, and troubleshooting tickets, required organizational skills beyond the purely technical. I developed a workflow using checklists and version-control notes to make sure nothing fell through the cracks. By the final week, I could handle overlapping tasks more efficiently, which proved to me that technical expertise must be supported by good planning.

The learning curve for enterprise-levels tools was steep. Cisco's interface ecosystem, SD-WAN orchestration, and firewall policy syntax were intimidating at first. That challenge became something I'm proud of. Each time I figured out an unfamiliar log entry or fixed a configuration warning, I felt myself getting better. The process reinforced an important professional truth: competence comes from pushing through discomfort and leaning into complexity rather than avoiding it.

10. Recommendations for Future Interns

For students who follow in my footsteps at Cavalier Logistics, my first recommendation is to show up with strong foundational knowledge of networking principles. Understanding subnets, VLANs, routing tables, and OSI layers will make on-the-job learning much smoother. If you can read and interpret network diagrams, you'll gain credibility. It's also worth getting familiar with

Cisco networking environments beforehand. Exploring free Cisco Networking Academy courses before starting would be really helpful.

I'd also recommend developing soft skills alongside technical ones. My most successful moments during the internship happened when I combined technical knowledge with being able to communicate clearly. Learning how to summarize findings for managers, creating accurate reports, and being knowledgeable about cybersecurity concepts is a great way to put yourself ahead of other interns too.

Approach every assignment with curiosity and humility. Some tasks, like labeling cables or organizing documentation, might seem trivial, but they're crucial to maintain system organization. Treating small duties with the same care as high-profile projects show reliability and earns your mentor's trust. Ask for feedback regularly, and when you hit limitations, use them as opportunities for independent research. Setting up a home lab or simulation environment can help you practice what you observe on site.

Future interns should take ethical responsibility seriously. At Cavalier Logistics, even routing network access involves sensitive client information. Understanding confidentiality agreements, documenting changes accurately, and avoiding shortcuts are non-negotiable. Your integrity builds your reputation; one careless action can undo months of clever work. Those who treat cybersecurity not just as technology but as a professional ethic will do well in this environment.

11. Conclusion

Looking back on my internship at Cavalier Logistics, I see it as a defining chapter in my academic and professional journey. It transformed classroom lessons into lived experience, showing me how cybersecurity protects what keeps modern businesses running, which is data and connectivity. I came in eager to learn about network security; I left understanding that security is the foundation supporting every organization process. Through exposure to Cisco technologies, SD-WAN architecture, and cloud management, I gained not only technical competence but also strategic awareness of how business and cybersecurity work together.

The biggest takeaway is that effective security is holistic. It depends equally on systems, people, and policies. The internship shows me how leadership, documentation, and communication reinforce technical defenses. It also deepened my appreciation for how different departments work together such as logistics specialists, accountants, and IT engineers all rely on one another's precision. This insight has reshaped how I view my education at Old Dominion University. I now see my courses not as isolated courses or subjects, but as connected pieces of a larger professional picture.

As I continue my studies, I plan to focus on courses that combine data analytics, risk management and digital forensics. I am also pursuing certifications such as Certified Fraud

Examiner (CFE) and Cisco Certified Network Associate (CCNA) to strengthen both my technical and investigative credentials. The internship confirmed my ambition to build a career that combines cybersecurity with forensic accounting which would be an area where I can help organizations detect, prevent, and analyze digital financial crimes.

This experience has reinforced my belief that cybersecurity is more than a career path; it is a commitment to protecting trust and organizational resilience. The lessons that I learned at Cavalier Logistics such as discipline, adaptability, and ethical integrity will continue to guide my academic work and professional conduct. I now see every configuration, audit, or report not as a routine task but as a contribution to a safer and more transparent digital world. The internship did not just teach me how to protect networks, it taught me how to think like someone responsible for protecting information, a perspective that will shape every step of my future career.