Date: April, 2025

Student Name: Yohannes Teklu

Employer: Mare Non-Emergency Medical Transportation

Company/Agency: Mare Transportation Services, Midlothian, VA

Internship Class: CYSE 368/Internship

Term: Spring 2025

Final Internship Report

Table of Contents

1. Introduction

Mare Non-Emergency Medical Transportation was the company I chose to intern with because it gave me a chance to combine my technical skills with important volunteer work. I want to get a degree in cybersecurity, so this job gave me a chance to see how IT systems help with important health services in the real world. Transportation for patients to non-emergency medical appointments needs to be efficient, keep data private, and be dependable. These are all places where cybersecurity plays a big role.

Three main goals I wanted to reach were: (1) get better at technical troubleshooting and diagnosis in a real-world setting; (2) learn how to work with IT teams and end users; and (3) learn how cybersecurity frameworks and controls are used in small to medium-sized businesses. I worked closely with several different systems during my internship and learned how to find the right balance between technical efficiency and user experience.

This report outlines my 150-hour internship at Mare Transportation, focusing on the skills I learned, the problems I faced, and how this experience helped me grow professionally and academically.

2. Organization Background and Internship Onboarding

Mare Non-Emergency Medical Transportation is a Midlothian, Virginia-based private service provider. Offering non-emergency transport services to those who need help traveling to medical facilities is its area of expertise. Senior citizens, those with impairments, and patients with long-term conditions who need routine care but do not require emergency care are among its target groups.

By reducing missed medical appointments among underprivileged communities, the organization aims to indirectly benefit public health systems. It offers door-to-door transportation, real-time dispatch assistance, and collaboration with medical providers.

I took part in a two-day orientation at the start of my internship, which covered the managerial and dispatch offices, Mare Transportation's mission and values, and the organizational structure. The IT orientation includes a tour of the ticketing systems, user management interfaces, help desk environment, and important cybersecurity regulations.

I was provided with a workstation and access credentials to various platforms, such as the internal communication system, ServiceNow (which is used for ticketing), and Active Directory with restricted administrative privileges. I had a good first impression of the company. IT integrity and service excellence were clearly prioritized, and the staff was friendly. The openness of the onboarding process and the organized training that equipped me to make a significant contribution right away were really appreciated.

3. Management Environment

Mare Transportation's management structure was efficient despite being somewhat flat. The IT Administrator, who was my immediate supervisor, and one support technician comprised the small IT department. Regular task evaluations, daily check-ins, and close mentoring were made possible by this framework.

Consistent supervision was provided without being intrusive. In addition to encouraging me to take responsibility for tickets and projects, the IT administrator gave me helpful criticism that raised the caliber of my work. The decision-making process was cooperative, and my suggestions for technical adjustments or little enhancements were frequently taken into account.

End-user happiness, responsibility, and communication were prioritized in the larger management context. Despite the company's lack of resources, the team handled user requests and technical limitations with professionalism and inventiveness. My exposure to this management style gave me the confidence to follow protocols and independently come up with solutions.

4. Major Work Duties and Projects

As part of my job, I worked on a variety of IT support tasks, from fixing common problems to designing and implementing larger projects. Daily tasks mostly included fixing hardware and software problems, handling requests for user access, setting up new workstations for employees, and helping areas with other system-related issues. These duties made sure that the business kept running, especially by keeping the tools for communicating between the dispatch team and healthcare providers available.

On a daily basis, I used ServiceNow to keep track of and record support tickets. Technical problems I dealt with included printer connectivity issues, Microsoft Outlook mistakes, VPN connection drops, and access control lockouts. Utilizing Microsoft's Remote Desktop tools, I could effectively help users from various areas without having to be present in person.

I helped with a big job that involved imaging, setting up, and deploying 10 new Windows workstations. Each device is pre-installed with standard apps, security fixes, endpoint protection, and Active Directory domain settings. I wrote down each step of the installation process and added it to the company's internal information base.

5. Application for Cybersecurity Skills

I had multiple chances to put the cybersecurity information I learned in class and via my certifications to use during my internship. By looking over event logs and endpoint security warnings, I helped keep an eye out for possible security incidents. I also saw how antivirus software and patch management contributed to endpoint security.

The idea of least privilege was one very pertinent skill I used. I made sure that user permissions were suitable for their work roles using Active Directory—neither more nor less. Additionally, I assisted in enforcing the password complexity, expiration, and account lockout policies—all fundamental yet essential security measures.

I had previously taken classes like CYSE 200T and Security+ that taught me about typical threat vectors and security principles before the internship. But this internship gave me a better understanding of how these ideas are used in limited settings. For example, I discovered how to use open-source technologies and simple Windows rules to safeguard systems on a budget.

I also learned more about cybersecurity incident response, specifically how to report phishing emails, disable compromised accounts, and record the response procedure for future use.

6. ODU Curriculum Preparation

The cybersecurity classes at Old Dominion University helped me a lot with my job at Mare Non-Emergency Medical Transportation. The things I learned in several classes directly applied to the work I did and helped me see how my duties fit into the bigger picture of corporate cybersecurity.

In particular, CYSE 200T made me more aware of how cybersecurity is more than just professional skills; it also has social, legal, and moral aspects. This class taught me more about ideas than about how to do things. It made me more responsible and aware in my work, especially when I had to deal with user data and private medical data. How I handled user credentials and enforced security rules was based on how I understood how compliance frameworks and ethics interact with technology.

And classes like CYSE 270 (Linux System Administration) and CYSE 280 (Windows System Management) let me learn how to use operating systems and oversee system processes by doing them myself. These professional skills were used directly when setting up the system, setting up user accounts, and fixing problems with hardware and software.

The work I had to do also taught me how to properly record things and talk to people clearly. Writing technical documentation, like the standard operating procedures I had to write, felt like

something I had done before because previous tasks had stressed clarity and structure. The communication skills I worked on in class during presentations and peer reviews gave me confidence when helping end users or talking to managers about technical issues.

Also, the theoretical information I learned in class through homework, group discussions, and lab work helped me a lot when I had to understand security policies, do audits, or look at the best ways to protect networks. I was able to use ideas like layered defense, risk analysis, and vulnerability studies in the real world thanks to the internship. This hands-on learning made me realize how important my academic background was while also showing me how to make decisions and solve problems in a professional IT setting.

7. Evaluation of Internship Learning Objectives

Three main learning objectives were outlined in the introduction: (1) developing practical troubleshooting abilities, (2) obtaining professional IT support experience, and (3) comprehending how cybersecurity principles are applied in real-world settings. After 150 hours, I can state with confidence that all three goals were accomplished.

First of all, I became much better at troubleshooting. I was able to more successfully discover, isolate, and fix issues by working closely with end users. Using diagnostic tools, asking the correct questions, and remaining calm even when problems got out of hand were all skills I acquired. I developed a stronger technical foundation as a result of each challenge, which increased my confidence and effectiveness while taking on new tasks.

Second, the internship gave me a firsthand look at a professional IT support environment. Daily

check-ins and urgent ticket resolutions taught me how to handle several requests while still providing high-quality service. I gained valuable professional communication, time management, and customer service skills, all of which are vital in any technical support setting. Just as valuable as the technical challenges were the administrative and interpersonal experiences.

Third, I was able to observe cybersecurity concepts in operation. I have direct experience with how security frameworks are implemented in small businesses, particularly in situations with limited funding. This involved establishing access controls, comprehending risk prioritization, and assisting with the documentation of compliance procedures. Beyond what the classroom could offer, these teachings improved my understanding of cybersecurity dynamics in the real world.

All things considered, the internship not only fulfilled but surpassed my expectations by fusing professional development with technological application and providing a more comprehensive understanding of how cybersecurity works across corporate operations.

8. Most Motivating Aspects of the Internship

One of the most inspiring things about my job was seeing how my work changed things. As I fixed a problem, whether it was restoring a dispatcher's workstation, fixing an application bug, or helping an employee get back into their account, I knew that I was directly helping people get healthcare.

With this sense of real-world meaning, I was able to keep working, even when the tasks got boring or hard to do. Making someone else's job easier and getting praise from both users and supervisors made me feel important and motivated me to keep learning.

Also, being able to work on some projects on my own made me feel safe. Taking charge of setting up workstations and writing up things was fun for me, and being able to lead smaller projects made me feel more confident and responsible.

9. Most Discouraging Aspects of the Internship

The job was generally a good experience, but there were some frustrating parts. It was especially disheartening to deal with old technology. Multiple devices had outdated operating systems, weren't getting regular patches, or had hardware problems that made it take a long time to do even the most basic things.

Additionally, some internal processes were not well recorded, which caused confusion and unnecessary work to be done twice. Questioning procedures over and over again slowed me down in the beginning and made me feel unsure at times.

Dealing with resistance from users when enforcing security rules was another worrying factor. Users sometimes found strict password rules or multi-factor authentication annoying, which made it harder to enforce best practices.

After hearing these negative comments, I decided to see them as opportunities to learn—reminders that part of an IT professional's job is to support both system security and user education.

10. Most Challenging Aspects of the Internship

The hardest part of my internship was dealing with a lot of technical problems at once in a fast-paced workplace. Quite often, I had to handle several tickets at the same time, each with a different amount of importance. A steep but rewarding learning curve helped me learn how to organize tickets, let people know about delays, and fix problems while under a lot of stress.

Another problem was fitting in as a student in a professional IT setting. Even though I had learned things in class, I had to be flexible to make them fit the needs of the job and the way things were set up. In real life, not every answer in the textbook worked perfectly. Sometimes I had to get creative and do research to find answers that did work.

Finally, it was hard at first to keep good communication going with both expert and non-technical users. Learning how to translate technical terms into easy-to-understand words took some time, especially when working with medical staff who didn't know what IT terms meant.

11. Recommendations for Future Interns

These suggestions will help future interns get the most out of this experience:

- Practice basic system management and troubleshooting: Understand how to use popular diagnostic tools, get around in Windows environments, and connect to networks properly.

- Examine Active Directory and the steps for managing users: Learning about group rules, user provisioning, and how to reset passwords will make onboarding go more smoothly.
- Focus on improving your communication skills by learning how to explain complicated issues in simple language and by actively listening to users when you work with them.
- Learn as much as you can by exploring new tools, asking questions, and volunteering for jobs that are outside of your comfort zone.
- Archive information: Writing down everything you learn is important. In addition to helping, you grow; this could also help future interns who may find your notes useful.
- Be flexible and patient: Information technology help in the real world isn't always reliable. Get better at staying calm, setting priorities, and dealing with stress in a healthy way.

12. Conclusion

When I think back on my 150-hour job, I'm proud of how far I've come professionally and technically. As an IT support and cybersecurity professional, my time at Mare Non-Emergency Medical Transportation has taught me what it means to work for a mission-driven company.

This job gave me a chance to use what I had learned in school in a real-life setting. It also made me more confident in my ability to fix problems and help users, and it made me more interested in how cybersecurity is used in real life. It also gave me the chance to learn skills that you can't learn in a classroom, like how to deal with stress, work with others, and make solutions fit the needs of a specific company.

As I get ready to graduate, I will remember the things I learned during this journey. I feel like I'm better prepared for entry-level jobs in cybersecurity, systems administration, or IT support, and I want to get more training and experience that will help me get even better. I'm grateful for the guidance, trust, and support I got during this internship, and I can't wait to use what I learned as I move up in my work.