CYSE 368 Internship Final Reflection Paper

Envision Holdings Group LLC

Cora Wilson

Employer: Cristina Carroll, Director of Operations

Company/Agency: Envision Holdings Group LLC

Instructor: Professor Teresa Duvall

CYSE 368 / Internship

Summer 2026

August 9, 2026

Table of Contents

1. Introduction

I decided to pursue my internship with Envision Holdings Group LLC because it offered something that many cybersecurity internships do not: the chance to build an IT and information security function from the ground up inside a small, growing company. CYSE 368 is a required capstone course for the Bachelor of Science in Cybersecurity program at Old Dominion University, and it is designed to serve as the culminating, real-world experience that ties together everything a student has studied throughout the degree. When I learned that Envision Holdings Group was looking for an intern who could take ownership of help desk support, documentation, and information security initiatives, I saw an opportunity to apply my coursework directly to a live business environment rather than a simulated one. This paper reflects on my full three-hundred-hour internship experience, from my first day of orientation through the completion of my final reflection, and discusses how that experience shaped my technical skills, my professional identity, and my future within the cybersecurity field.

My signed Memorandum of Agreement (MOA) with my supervisor, Cristina Carroll, established four primary learning objectives for the internship: IT help desk support, Standard Operating Procedure (SOP) development, asset tracking and management, and information security support. I hoped that by the end of the internship I would be able to independently manage a functioning help desk system, produce professional-quality security documentation, maintain an accurate inventory of company technology assets, and contribute meaningfully to the organization's overall security posture. I also hoped, on a more personal level, to determine whether I was better suited to a technical or a policy-driven path within cybersecurity, and to gain the workplace confidence that only comes from real accountability.

Envision Holdings Group LLC is a growing company based in Winchester, Virginia, in the Shenandoah Valley, that operates across real estate, construction, design, land development, and lending services. The company works with homebuyers, property owners, investors, and vacation rental guests throughout the region, and it has continued to expand its operations and staff since it was founded. Because the company was growing quickly and relied on a hybrid and partially remote workforce, leadership recognized a need for a more structured internal IT presence and dedicated information security practices. That need is what created the IT/Cybersecurity Intern position I was hired into, and it is part of what made the internship such a valuable experience. Rather than stepping into an already mature IT department, I was often the person building the processes and systems that the company would use going forward.

My orientation and initial training consisted of meeting directly with Cristina Carroll, the Director of Operations, who would serve as my supervisor throughout the internship. During my first days, I was introduced to the rest of the team, given access to company systems and equipment, and briefed on the company's current technology environment, including the devices, software, and informal processes already in place. I remember feeling a mix of excitement and nervousness, since I understood that I would be one of the first people at the company focused specifically on IT support and cybersecurity. My initial impression was that Envision Holdings Group was a close-knit, fast-moving organization where employees were used to solving problems independently, which meant there was a real opportunity for me to add value quickly if I was willing to take initiative. That first impression turned out to be accurate, and it shaped how I approached the rest of my internship: proactively, and with a willingness to build structure where none existed before.

2. Management Environment

The management environment at Envision Holdings Group was defined by a flat, hands-on structure and a high degree of trust between employees and leadership. My direct supervisor, Cristina Carroll, Director of Operations, oversaw my day-to-day responsibilities, but the company as a whole operated with relatively few layers of management, which meant that decisions moved quickly and employees at every level, including interns, were expected to take ownership of their work. From the beginning of my internship, Cristina made it clear that she trusted me to manage many of my responsibilities independently while remaining available whenever I needed guidance, clarification, or feedback.

This balance between independence and support proved to be one of the most effective aspects of the management structure. Rather than being micromanaged through every task, I was encouraged to research solutions on my own, make recommendations, and bring completed work back for review. At the same time, I never felt unsupported. Whenever I encountered a challenge, I could not resolve on my own, whether it involved a technical issue or a question about company policy, I knew I could reach out to my supervisor or to another cybersecurity professional within the company who occasionally collaborated with me on planning and security discussions.

One specific example of the management style's effectiveness was my inclusion in the company's weekly meetings. I requested to be added to these meetings because I wanted a better understanding of how communication and decision-making functioned across the organization, and my request was welcomed without hesitation. Being included in these discussions gave me insight into how leadership prioritized projects, addressed challenges, and communicated expectations to the broader team, and it reflected a management culture that valued transparency and employee development rather than limiting information to senior staff.

Overall, I found the management environment at Envision Holdings Group to be highly effective for someone in an internship role. The autonomy I was given allowed me to grow quickly and take ownership of meaningful projects, while the accessibility of my supervisor and colleagues ensured that I was never left to struggle without support. This management approach built my confidence, encouraged accountability, and prepared me for the level of independence expected of a full-time cybersecurity professional.

3. Major Duties, Assignments, and Projects

Throughout my internship, my duties expanded significantly as I demonstrated reliability and technical competence. My earliest and most consistent duty was managing the company's IT help desk. At my supervisor's request, I researched and implemented Spiceworks as a ticketing and asset management platform, set up a dedicated help desk email address, and configured the system so that employee support requests were routed directly to me. This gave the company, for the first time, an organized and trackable way to manage technical support requests rather than relying on informal, ad hoc communication. This duty is necessary for the business because as the company grows and adds employees across multiple locations, unresolved or poorly tracked technical issues can quickly reduce productivity and increase security risk.

A closely related responsibility was asset tracking and inventory management. Using the same Spiceworks platform, I documented every company device, including serial numbers, manufacturers, and assigned users, and built a centralized system for tracking the condition and location of company equipment. This project matters to the business because an organization cannot secure or maintain what it cannot account for; accurate asset records are the foundation of both efficient IT operations and effective cybersecurity, since every unmanaged device represents a potential vulnerability.

I also spent a substantial portion of my internship developing Standard Operating Procedures (SOPs) covering topics such as password security, phishing awareness, device management, acceptable use, and remote work technology guidelines. Later in the internship, I expanded this work into drafting the technical sections of the company's employee handbook, including onboarding guides and best practices for maintaining secure systems. This documentation is essential to the business because it establishes consistent expectations for all

employees, reduces the organization's risk exposure, and ensures that security practices do not depend solely on informal knowledge held by any one person.

One of the most significant projects I worked on was researching and delivering a presentation to the company's CEO on cybersecurity awareness and account security. This project required me to research common phishing tactics and employee awareness training strategies, as well as evaluate multi-factor authentication (MFA) solutions, recommending Cisco Duo as a potential platform for the organization. This work is critical to the business because credential theft and phishing remain some of the most common ways organizations are compromised, and gaining executive buy-in for MFA and awareness training directly reduces that risk.

Building on that research, I was later given the responsibility of purchasing and deploying a company-wide Norton Antivirus solution, coordinating its distribution so that employee devices across the organization were protected. I also took on both the offboarding of a terminated employee and the onboarding of a new employee, which involved archiving company data, securing, and disabling accounts, wiping, and preparing equipment for reuse, and configuring new accounts, permissions, and workstations. These account lifecycle responsibilities are vital to the business because improperly offboarded accounts and devices represent one of the most common sources of data breaches and insider risk, while a smooth onboarding process ensures new employees can be productive and secure from their very first day.

Finally, I was given the opportunity to collaborate with a cybersecurity consultant based in Brazil on scripting and coding related to the company's artificial intelligence initiatives. While this project was still developing by the end of my internship, it exposed me to how cybersecurity and software development intersect with emerging technology, and it represents the kind of forward-looking work that helps the business remain competitive as it integrates AI into its operations.

4. Application of Cybersecurity Skills and Knowledge

Before beginning my internship, my cybersecurity education had given me a solid foundation in areas such as cybersecurity fundamentals, systems security, risk management, networking, information assurance, and cybersecurity policy. I understood core concepts like the importance of layered security, the fundamentals of authentication, and the principles behind risk assessment and mitigation. However, most of this knowledge existed at a conceptual or academic level, built through coursework, labs, and case studies rather than through direct responsibility for a real organization's security posture.

My internship required me to translate that theoretical knowledge into practical, on-the-job execution. I had to learn how to operate a real ticketing and asset management platform, configure remote support tools, and manage a live inventory of company devices, none of which had been directly taught in my coursework. I also had to learn how to evaluate and select actual security vendors and products, including researching Cisco Duo for multi-factor authentication and Norton Antivirus for endpoint protection, and then manage the real-world logistics of purchasing, licensing, and deploying those solutions across the organization. Writing SOPs and handbook content that real employees would follow required a different skill than writing a policy paper for a class; it demanded clarity, practicality, and an understanding of how non-technical employees would interpret my instructions.

I also developed skills I had never been required to use in an academic setting, including securely offboarding and onboarding employee accounts and equipment, presenting cybersecurity recommendations directly to executive leadership, and beginning to explore how artificial intelligence and coding intersect with cybersecurity through my collaboration with a colleague in Brazil. These experiences taught me that cybersecurity work is rarely just technical; it constantly

requires communication, documentation, and judgment to call that textbooks cannot fully prepare you for.

This internship changed my understanding of cybersecurity by showing me that the field is fundamentally sociotechnical. Strong technical knowledge is necessary, but it is not sufficient on its own. Being able to communicate security concepts to non-technical employees, write documentation that people will use, and make sound decisions when supervision is limited are just as important as understanding the underlying technology. I now see cybersecurity less as a set of isolated technical tools and more as an ongoing organizational practice that depends on people, processes, and technology working together.

5. Preparation from the ODU Curriculum

My coursework at Old Dominion University's School of Cybersecurity provided a strong conceptual foundation that connected directly to much of the work I performed during my internship. Courses covering cybersecurity fundamentals, risk management, information assurance, systems administration, cybersecurity policy, and network security all contributed to my ability to understand and contribute to the projects I was assigned. For example, my coursework in risk management helped me understand why asset tracking and inventory management are foundational to an organization's security posture, and my exposure to cybersecurity policy coursework directly informed my approach to writing SOPs and handbook documentation.

Several experiences during my internship reinforced concepts I had already learned in school. My understanding of phishing, social engineering, and the importance of multi-factor authentication, all covered in my coursework, was reinforced when I researched and recommended Cisco Duo to company leadership. Similarly, my academic exposure to endpoint security concepts made it easier for me to evaluate and select an antivirus solution for the organization, since I already understood what that category of tool was meant to accomplish, even though I had not previously been responsible for purchasing and deploying one myself.

At the same time, my internship revealed several concepts, tools, and skills that I had not yet encountered in my formal coursework. I had never used a real IT ticketing and asset management platform like Spiceworks, nor had I been responsible for the practical coordination of vendor selection, procurement, and deployment of a security solution across an entire organization. My coursework also had not prepared me for the realities of employee account lifecycle management, including the sensitive, security-critical process of offboarding a terminated employee. Presenting cybersecurity recommendations directly to a CEO was another experience

with no direct classroom equivalent; it required me to distill technical research into a clear, business-focused recommendation for a non-technical decision-maker. Finally, my brief exposure to scripting and artificial intelligence through my collaboration with a colleague in Brazil introduced me to a technical area that my degree program had only touched on briefly, and it showed me how much opportunity exists at the intersection of cybersecurity and AI.

Overall, my ODU curriculum gave me the conceptual vocabulary and foundational knowledge I needed to understand and contribute to my internship responsibilities from day one, even though many of the specific tools, workflows, and interpersonal demands of the job could only be learned through direct experience.

6. Fulfillment of Internship Learning Objectives

My signed MOA established four primary learning objectives for this internship: IT help desk support, SOP development, asset tracking and management, and information security support. Reflecting on my full three hundred hours at Envision Holdings Group, I believe each of these objectives was not only fulfilled but exceeded.

The objective of IT help desk support was fulfilled through my work establishing and running the company's help desk system. I researched and implemented Spiceworks, created a dedicated help desk email address, and became the primary point of contact for employee technical support requests. Over time, I also configured remote support capabilities, allowing me to assist employees regardless of their location. By the end of my internship, I had a fully functioning, organized help desk process where none had existed before.

The SOP development objective was fulfilled through the creation of multiple Standard Operating Procedures covering password security, phishing awareness, device management, acceptable use, and remote work technology, as well as my later contributions to the technical sections of the company's employee handbook. This body of documentation gave the organization consistent, written security expectations that will continue to be used long after my internship concludes.

The asset tracking and management objective was fulfilled through my work building out the company's technology inventory within Spiceworks. I documented company devices, tracked assigned users, and created an organized system for monitoring the condition and location of equipment, giving the company visibility into its technology assets that it had not previously had in a centralized, trackable form.

Finally, the information security support objective was fulfilled, and in many ways exceeded, through my work researching and recommending multi-factor authentication solutions, presenting cybersecurity awareness recommendations to the CEO, purchasing and deploying a company-wide antivirus solution, and securely managing the offboarding and onboarding of employee accounts and equipment. Each of these projects directly strengthened the organization's security posture and gave me hands-on experience across every category of information security work outlined in my learning objectives.

7. Most Motivating and Exciting Aspects

The most motivating aspect of my internship was the trust that my supervisor and colleagues placed in me throughout the experience. Being given independence to research solutions, making recommendations, and managing entire projects, such as the company's help desk system and its employee handbook, gave me a genuine sense of ownership over my work. Knowing that my contributions were making a real difference in the organization, rather than functioning as a simulated academic exercise, kept me engaged and motivated even during more repetitive or administrative tasks.

Being invited to participate in the company's weekly meetings was another exciting development, since it gave me exposure to workplace communication and decision-making that I could not have gained simply by completing my assigned tasks. I found it exciting to watch how the organization prioritized projects and addressed challenges, and being included in that process made me feel like a genuine member of the team rather than just an intern completing hours.

I was also excited by the opportunity to begin collaborating with a cybersecurity consultant based in Brazil on scripting and artificial intelligence initiatives. This experience introduced a global, technical dimension to my internship that I had not expected, and it motivated me to continue developing my coding and AI-related skills beyond what my coursework had covered. Presenting my cybersecurity research and recommendations directly to the company's CEO was similarly exciting, as it gave me a rare opportunity as a student to influence real organizational decisions.

By far, the most motivating moment of my entire internship came to its conclusion, when I received an official job offer from Envision Holdings Group to continue working for the company after completing my internship hours. That offer confirmed that the work I had contributed over

the previous months had real value to the organization, and it remains one of the proudest accomplishments of my academic and professional career so far.

8. Most Discouraging Aspects

While my internship was overwhelmingly positive, there were aspects of the experience that I found genuinely discouraging. The most significant of these was the sheer volume of the workload relative to the time I had available. Completing three hundred internship hours while managing coursework, personal responsibilities, and an increasingly demanding set of duties, ranging from help desk support to SOP development to security research, required a level of time management that was, at times, difficult to sustain. There were periods where the number of concurrent projects made it hard to feel like I was giving each responsibility the attention it deserved.

Related to the workload, I found it genuinely difficult at times to separate my personal life from my work life. Because I was often trusted to work independently and manage my own schedule, the boundary between "internship time" and personal time could blur, especially during weeks with heavier responsibilities. Learning to protect time for rest and personal responsibilities, rather than allowing the internship to expand into every available hour, was a real and sometimes discouraging challenge, even though it became an important lesson in professional sustainability.

Finally, the unpaid status of the internship was a discouraging aspect of the experience, particularly as my responsibilities grew to include tasks with real financial and operational impact for the company, such as purchasing security software and managing sensitive employee account transitions. Contributing at that level while unpaid was, at times, difficult to reconcile, and it was part of what motivated me to eventually raise the possibility of transitioning to a paid position with my supervisor. While I understood the educational purpose of the unpaid internship structure, the financial reality of dedicating so many hours to unpaid work were a real and valid source of discouragement during the experience.

9. Most Challenging Aspects

The most challenging aspect of my internship was adjusting from the classroom's structured, guided environment to a professional setting where I was expected to identify problems, research solutions, and act with minimal direct oversight. Early in the internship, I often had to learn entirely new tools and platforms, such as Spiceworks, remote support software, and vendor evaluation processes for products like Cisco Duo and Norton Antivirus, on my own, without a formal training program to guide me. Figuring out how to teach myself unfamiliar systems while still delivering reliable results for a significant business was, at times, intimidating.

Another significant challenge was communicating technical concepts clearly to people with varying levels of technical background, ranging from employees submitting help desk tickets to the company's CEO during my cybersecurity presentation. Translating technical research into a language that a non-technical audience could understand and act on required a different kind of skill than anything I had practiced in a classroom setting, and it took deliberate effort to develop.

I also found it challenging to prioritize effectively when I was responsible for multiple significant projects at once, including ongoing help desk support, SOP and handbook development, asset management, and, later, account offboarding and onboarding responsibilities. Determining which tasks needed immediate attention and which could be scheduled for later required judgment that I had to develop through experience rather than instruction.

Finally, offboarding a terminated employee was one of the most sensitive and challenging tasks I completed during my internship. Securing accounts, archiving data, and wiping company equipment required precision and discretion, since any mistake could have exposed sensitive information or disrupted business operations. Successfully navigating that process reinforced how much responsibility is placed on cybersecurity professionals during moments of organizational

change, and it pushed me to approach my work with a level of care and seriousness that I had not previously had to apply.

10. Recommendations for Future Interns

For future students considering an internship like mine, my first recommendation is to prepare financially and logistically for the possibility that the position may be unpaid, at least initially. Understanding this in advance can help reduce the discouragement that comes from balancing significant responsibility with no immediate compensation, and it allows students to plan their schedules and finances accordingly before the internship begins.

Second, I recommend that future interns strengthen their foundational IT support and technical writing skills before starting. Familiarity with common ticketing and asset management platforms, basic troubleshooting procedures, and the fundamentals of clear, professional documentation will make the transition into real responsibilities much smoother. Many of the tools I used, such as Spiceworks, MFA platforms like Cisco Duo, and antivirus solutions like Norton, are common across small and mid-sized organizations, so gaining even a basic familiarity with these categories of tools in advance would be valuable.

Third, I strongly encourage future interns to be proactive rather than waiting to be given responsibility. Some of the most valuable experiences I had, including my participation in weekly company meetings and my collaboration with an international colleague on AI-related projects, came about because I specifically asked to be included. Taking initiative and expressing genuine curiosity signals to supervisors that an intern is ready for greater responsibility.

Fourth, I recommend establishing clear boundaries between work and personal time as early as possible. Because internships like this often come with a high degree of independence, it is easy to let the workload expand into personal time. Setting clear expectations for yourself from the beginning will help prevent burnout over the course of a multi-month internship.

Finally, I recommend that future interns communicate regularly and openly with their supervisors, ask questions whenever something is unclear, and approach every new responsibility as a learning opportunity rather than a test to be passed. Cybersecurity and IT environments change constantly, and the willingness to stay curious and adaptable will serve future interns just as it served me throughout this experience.

11. Conclusion

Looking back on my full internship experience with Envision Holdings Group, my main takeaway is that cybersecurity work is as much about people, communication, and organizational trust as it is about technology. I began this internship hoping to develop technical competence in help desk support, documentation, asset management, and information security, and while I did develop strong technical skills in each of these areas, the most lasting lessons I learned were about professionalism, initiative, and the importance of clear communication with both technical and non-technical audiences. I am proud of everything I built during this internship, from the company's first organized help desk and asset management system to its technical employee handbook and its expanded endpoint security protections.

This experience will influence the remainder of my time at Old Dominion University by giving me a clearer sense of direction for my final courses and any additional certifications or electives I pursue. Having seen firsthand how cybersecurity policy, technical support, and emerging technologies like artificial intelligence intersect within a real organization, I intend to seek out opportunities in my remaining coursework that deepen my technical skills, particularly around scripting, automation, and security tool evaluation, while continuing to value the policy and communication side of the field that this internship showed me is equally essential.

Most significantly, this internship will directly influence my professional path going forward. Receiving a formal job offer from Envision Holdings Group to continue my employment after completing my internship hours was the clearest possible confirmation that the work I contributed had real value, and I plan to continue growing with the company as I finish my degree and begin my career. This experience gave me the confidence to know that I am prepared to contribute meaningfully to a real organization's cybersecurity and IT operations, and it has shaped

my professional goals around continuing to build technical expertise while never losing sight of the communication, documentation, and trust that make cybersecurity work effective in practice.