Student: Alexander Kotzian

Class: CYSE 368 Internships in Cybersecurity

Semester: Spring 2026

Date: 04/19/2026

Employer: A Better Way Campaign

Supervisor: Dharshini Senthil Nathan

Internship Title: Cybersecurity Specialist

Professor: Teresa Duvall

TA: Joshua Russell

Table of Contents

1. Introduction [Page 2]
2. Learning Objectives [Page 3]
3. Management Environment [Page 3]
4. Work Duties [Pages 4 - 6]
5. Cybersecurity Skills Used [Page 7]
6. How Old Dominion University Prepared Me [Page 8]
7. Learning Outcomes [Page 9]
8. Emotional Aspects of the Internship [Page 10]
9. Recommendations for Future Interns [Page 11]
10. Conclusion Page [Page 11]

Introduction

This is a remote internship that was originally advertised on forums or social media such as Handshake and LinkedIn as a sister company rather than the organization I ended up interning at. I decided to take this internship as it was the only Cybersecurity specific internship that gave me an offer over the course of multiple years of applying. Prior to being accepted in, I was onboarded through a group call with the organization owner with other interns. According to the organization owner, this organization was created to work in tandem with his new political campaign for office in Florida, as the original organization I applied to called Resilience Inc. caused concern for his campaign. It did concern me to intern for a political organization given the current state of the political environment in the United States. During official onboarding, I orientated myself through videos provided on the backend site used, which was Striven. During this onboarding process I was introduced to the organization structure, and soon found out that I would be primarily assigned to internal cybersecurity improvements and development. During onboarding I was introduced to the system in which they expected us to conduct our communication, tasks, and documentation structure. We were expected to only communicate within Striven either by using the discussion feature, task commenting feature, or by responding to announcements. We also were expected to accomplish tasks through a task feature within Striven, this would allow you to see the details of an assigned task, when it was expected to be accomplished, who was involved in the task, a commenting feature, and you could designate the task as Open, On Hold, Done, or Canceled. This specific way of task management was an issue for me throughout the internship, as other staff members within the task would set the status to done only when a portion of the task if any was completed, effectively miscommunicating the status of the task to the rest of the staff members. We used a large shared google drive to access, modify, and create documentation for our tasks. After general onboarding was completed, we were assigned to onboard with our specific department and subdepartment. Interning for Cybersecurity, I onboarded with the Cybersecurity subdepartment which was under the Information Technology department. I had inquired about branching out to other teams within the Information Technology department such as game development, but I refrained as my time was preoccupied by being a full time college student, part time employee, and interning at a separate company in tandem. During our onboarding meeting with the Cybersecurity subdepartment we volunteered for teams depending on what we wanted to learn, or what our skills were best suited for. The Cybersecurity subdepartment lead structured the team system based on the SMART framework. SMART stands for Self-Governance, Monitoring, Assessments, Remediation, and Training. Given my specific experience and interest in penetration testing, I volunteered to the assessments team. The Cybersecurity team would typically have a meeting every week or every other week. These subsequent meetings would be very targeted for a specific team or project, making it partially redundant for many members to attend. The tasks would not typically include cooperation or coordination with other members in the other Cybersecurity teams. Each Cybersecurity team was given a unique google drive file to use throughout the internship.

Learning Objectives

Shortly after onboarding, within the memorandum of agreement I had my supervisor sign, I outlined four learning objectives I wished to accomplish for my internship. The first learning objective I wished to accomplish is to conduct effective penetration tests in a professional security environment. By this I wanted to apply my knowledge of penetration testing and ethical hacking to scan for vulnerabilities, develop a risk analysis, and learn how to conduct those within a team environment under a supervisor. My second learning objective was to apply identity and access management controls. I wanted to develop a system or use an already put in place system to give and restrict access and types of access depending on authority and relevance to specific departments. My third learning objective was to evaluate human-focused security risks. I wanted to evaluate and improve potential security concerns or vulnerabilities that were brought upon by staff members, such as phishing attacks or other social engineering attacks. My final learning objective was to communicate and document security initiatives clearly and concisely. My intention was to learn how to abide by organizational documentation procedures, and communicate with non-cybersecurity oriented staff members effectively. I expected each of these learning objectives to be fulfilled throughout the internship.

Management Environment

The management environment of A Better Way Campaign was incredibly simple. It was composed of a top down structure, in which the head of the organization had the most authority. A step down from him was the Executive Leadership & Administration branch. After which was specified authority for each department head, the departments being: Communications, Field Operations, Fundraising, Human Resources, Information Technology, Public Policy Development, Research and Data Analytics, Self-Governance, Web Development, Accounting, Staff Training, Software Development, and Federal & State Governance. Each department had a jurisdiction in which they had more authority, the Information Technology primarily oversaw technology related access, authentication, authorization, and more. Within each department was a subdivision that had more specific responsibilities. Within the Information Technology department, our subdepartments included: Information Technology Research, Google Assets, Striven Management, Game Development, App Development, Fundraising Development, and Cybersecurity, each with their own project or team manager. Within the Cybersecurity team, there were five different teams based on the SMART Cybersecurity framework, these teams were: Self-Governance, Monitoring, Assessments, Remediation, and Training. Within each of these teams we received specific tasks that the subteam was responsible for, the assessments team in particular received the most new members, so I and another subteam intern assumed responsibility of being good communicators for the rest of the team in regards to tasks, task updates, and general in-team communication. We constantly updated each other with new information or expectations for members of the team, and we conducted our own meetings to ensure an effective work environment. We were expected to research and review other subteams' progress to stay on the same page as each other within the Cybersecurity team.

Work Duties

I was instructed to keep any and all documents relating to the internship within the organization's shared google drive. Although I did not sign a non-disclosure agreement regarding this, out of respect for the organization I will refrain from referencing the final documentation, and focusing on my input to these works. The first few assignments were documentation assignments in which our team created multiple documents to outline plans for a multitude of future projects. These projects included: a phishing simulation plan, a multifactor authentication plan, and a security assessment. I wrote both initial plans for the multifactor authentication plan and the phishing simulation plan.

I will outline my contribution to the multifactor authentication plan. In this plan I described the purpose of the multifactor authentication system was meant to be used by all staff and prevent many human-focused attacks. I outlined the scope to prioritize implementing multifactor authentication to administrative accounts and higher classification access. I gave priority to enforce multifactor authentication for email systems, administration and privileged accounts, and cloud based services. I detailed some potential multifactor authentication methods, some of which being application based authentication methods such as Google authenticator, Microsoft authenticator, and DUO mobile. I additionally gave a failsafe authentication method in the event that an application-based authenticator was down, providing SMS-based authentication. I suggested that the rollout phases of the future project should be conducted in three phases. Phase 1 would target the Information Technology and Privileged accounts. In this phase we would expedite multifactor authentication. Additionally we would test the multifactor authentication tool we decided, and identify potential failures and concerns. Finally we would identify and solve and further login or compatibility issues with our system and multifactor authentications integration. Phase 2 would see a rollout to the rest of the staff. Phase 2 would have users register with the chosen multifactor authentication method. Staff members would have two to three weeks to register with the chosen multifactor authentication. If users failed to register, they would be sent continuous notifications over the grace period. Phase 3 would see our enforcement of multifactor authentication. Multifactor authentication would be required to access all applicable systems. Unenrolled users would be blocked from accessing said systems. The Information Technology department would oversee support for multifactor authentication for unregistered and future staff members. I outlined a few exceptions to multifactor authentication and how we should handle the bypassing of it. I suggested that multifactor authentication bypassing should be requested only, these requests would be accepted or denied by appropriate Information Technology or Cybersecurity department staff. Additionally these requests would need to be time-limited and documented, they would be further monitored and logged for future review. These would allow the Information Technology department to review consistent issues with the multifactor authentication system, and hold department members accountable for misuse of the bypass system. I then went on to describe our monitoring of multifactor authentication. I designated four metrics that would help us determine risk areas and usability concerns, these four metrics included: multifactor authentication enrollment, multifactor authentication-related login in issues, accounts that were locked out post-enforcement phase, and the number of multifactor authentication bypass requests. My next section was to outline the communication regarding the multifactor authentication rollout, I split this into two sections pre-rollout and post-rollout. Pre-rollout, users would be notified of the multifactor authentication expectations, users would be notified of the multifactor authentication

enforcement procedures, and finally users would be sent instructions on how to enroll with the decided multifactor authentication method. Post-rollout, we would communicate with users on their concerns with the multifactor authentication system and alleviate those concerns, multifactor authentication related failure solution instructions would be sent to staff members, and new users would be provided multifactor authentication onboarding instructions. My final section of the plan outlined my expected security impact of the plan's fulfillment. I concluded that it would reduce the likelihood of successful phishing attacks, limit unauthorized access of systems within the organization, and increase protection against credential-based attacks.

In my initial phishing simulation plan I described the plan's purpose to evaluate staff susceptibility to phishing attacks, while measuring click-through behavior and identifying potential gaps in staff security awareness. I outlined the scope of the simulation to apply to all staff within the organization, measuring staff members' emails linked to both Google drive and Striven. I then outlined what should be monitored, which I decided should be click-through rate, number of users who clicked the phishing link, click trends by department and role, and email addresses that were associated with a simulated phishing link click. I specified to not monitor collection of any information outside of the associated email. I did have great concern determining what should and shouldn't be monitored, as privacy is of utmost importance, and it requires a good balance between privacy and safety. If creating the plan today I would not monitor email addresses. Next I included some potential phishing methods including: emails impersonating executives of the organization, email-based advertisements, and emails impersonating Striven support. I then gave a guideline for the phishing email structure, it needed to include a greeting, proper branding based on the email type, urgency to click the provided link, and the phishing link. My next step was to describe the click tracking method we would be using. We would log when the link was clicked, it would log the unique link associated with a sent email, the user should then be redirected from the link to a security awareness page, and be notified the email was a part of the simulation. My next section described the methods used to collect metrics. We were to create a unique link per email sent, create a sheet to log each click by each link, and create a script that logs the link clicked and stores it into the sheet. I then wrote some ethical concerns regarding the plan which included, no staff members privacy shall be breached, results should only be available for review by appropriate Information Technology and Cybersecurity staff, individual results should not be disclosed, focus on aggregate results rather than individual results. My next portion of the plan was meant to outline our communication process, similar to that of the multifactor authentication plan; it had two parts, pre-simulation and post-simulation. Pre-simulation, we would receive informed consent from leadership, and privacy and ethical safeguards should be documented and enforced. Post-simulation, we would inform all staff that a phishing simulation was conducted, give a summary of the results of the phishing simulation, and provide a phishing awareness guide. My next section covered a follow-up to the phishing simulations. We were to target identified weak points in our Cybersecurity awareness training, review results to develop a superior future phishing simulation, and conduct incremental simulations to study progress over time. My final section covered the expected security impact of this plan. I concluded it would improve organization-wide security awareness, significantly reduce likelihood of successful phishing attacks, and document risk associated with phishing attacks.

Although I did not write an official report, I did conduct a partial security assessment. As I was unable to view who had access to what in the Google drive, I added to my multifactor authentication who should have access to what in the Google drive. After I created these two plans, my team was tasked with doing occasional vulnerability testing. Nothing unusual was found throughout these tests and it was a good way to put into practice my penetration testing skills.

Although not confirmed, I believe that leadership decided to replace the prospects of creating a phishing simulation, with the creation of a phishing assessment instead, at least for the time being. The phishing assessment was our first and only whole-group task in which a majority if not all of the team participated. The premise of the assessment was to create a questionnaire that would be graded to gauge the phishing awareness of the test-taker. It was also meant to teach the test-taker about different types of phishing including but not limited to, phishing emails, sms-phishing, application phishing and voice phishing. It was expected that each member of the team would contribute a few questions, answers, and potentially phishing examples. I contributed an application phishing example, and a multiple choice phishing question. My multiple choice question covered potential steps to take if an alleged member of Striven were to personally contact you. My example was of a Google drive document invite from an unrecognized sender that used official Google drive logos and branding. I decided to have the test taker identify each of the available red-flags in their answers. This was the project I was required to have the most communication for, and decided to conduct multiple meetings in regards to. This was my last major task for the internship, and I have yet to be assigned any more Cybersecurity related tasks as of this date.

In the meantime, I have been assigned a multitude of tasks related to the social media campaign under the organization. It is imperative to the success of the organization that social media is successful. Considering the organization is meant to run a political campaign exposure is of utmost priority for the organization. Regarding this, my most recent tasks have been to create social media accounts for: Facebook, Youtube, Instagram, X, and TikTok. I was only able to create private accounts for some of these. For the remainder of my internship it is my expectation that I will receive no more Cybersecurity tasks and will only be pushed to engage with the social media posts the organization has posted. I have reached out to the Cybersecurity team lead regarding this and have also had no response as of this date. In tandem with each post I am assigned a task to engage with said social media post, and report that I have engaged. I believe that a major reason for the lack of Cybersecurity tasks is that there has been a large number of staff members offboarded towards the end of the spring semester, as I have received many notifications of available leadership positions. For now I do not intend on seeking a leadership position as I am expected to finish my internship and graduate within the next month. I intend on seeking a paid position within Cybersecurity prior to ending my internship. With the experience from these projects I hope that I will seem more valuable as a candidate for future employers.

Cybersecurity Skills Used

Throughout this internship I had the opportunity to use many of the Cybersecurity skills I have learned throughout my experience in this career. A majority of these practical skills have come directly from my learning of them throughout my time at Old Dominion University, and the curriculum there. Considering my primary goals were to apply those skills, I can outline what I was able to put into practice. Going task by task, the multifactor authentication plan put to test my understanding of backend systems and the importance of authentication and authorization. Although I have not learned to implement a multifactor authentication prior to this internship, I have had to research potential implementations. I do wish my team and I were able to implement these systems as that would have given me incredibly valuable experience. However, creating a plan to implement multifactor authentication proves my experience in implementing the Confidentiality, Integrity, and Availability triad into practice. This triad is meant to provide a guideline for ensuring users are properly authorized for access, the data is available for access, and the information accessible is accurate. I was able to showcase my knowledge of the confidentiality portion of the triad during the creation of this plan. Additionally I was able to partially present my understanding of access controls and a tiered authentication system. I was also able to provide a specific step-by-step process that addressed all potential issues regarding the multifactor authentication system.

The phishing simulation plan allowed me to showcase my knowledge of the many types of human-focused attacks, primarily phishing. I was able to present my understanding of what makes phishing emails attractive, the red flags of one, and how to improve phishing awareness. The most important skill I was able to learn and showcase during this task was hypothesizing an entire simulation. The hallmarks of this simulation being a custom backend monitoring and logging system, and a custom link creation system to ensure a unique link per email. Each with addressing ethical concerns of a phishing simulation. Additionally I was able to develop a concise and informative plan to emphasize the process and aim of the phishing simulation. Although I wish my team and I were able to implement this simulation as it would have been incredibly fun, and put our phishing, scripting, and analysis skills to the test.

During my baseline vulnerability assessment of the Google drive section of our organization, I was able to confirm we accomplished the Integrity and Availability portions of the CIA triad. I confirmed the information was up to date, and available to access. I did bring concerns that I was unable to identify who had access to what files in the Google drive. I was eventually able to update the Google drive access information to my leadership after being given the authorization to view access. This task allowed me to showcase effective communication and inference regarding authorization and access controls.

During the consistent vulnerability testing I was able to showcase my skills using official penetration testing tools such as Nmap, Wireshark, and a tool suggested by the sister organization, WPScan. Each of these tools with the exception of WPScan, I have used numerous times in my Cybersecurity and penetration testing classes in Old Dominion University, so I was exceptionally prepared to accomplish this task.

How Old Dominion University Prepared Me

As stated in the previous section much of the Cybersecurity tools, techniques, and frameworks used throughout my internships I had been previously familiarized with through Old Dominion Universities curriculum. Starting with the multifactor authentication plan, I had learned how to structure a plan from previous writing classes for university. On top of this I learned the importance of tiered authentication through learning about the CIA triad and other frameworks in university. Additionally I was able to report expected security impacts based on inference and potential consequences of the plan.

For the phishing simulation plan I used my experience in conducting phishing simulations and metasploit attacks from university to outline a potential phishing simulation plan. In this plan I used my knowledge of how phishing attacks are typically structured and what they are aiming for in their attacks. On top of this I was able to perform ethical reasoning to determine the best plan. I would attribute my application of ethical reasoning to Cybersecurity Ethics class as well as my Philosophy courses.

The baseline assessment analyzing the Google drive access was reminiscent of learning of access controls, authorization, authentication, and classification systems learned in university. Additionally my use of Google drive throughout my academic career allowed me to navigate the Google drive efficiently and identify potential authorization issues quickly.

The consistent vulnerability tests are where most of my penetration testing curriculum from university applied. My prior knowledge of Nmap allowed me to effectively and quickly scan for potential vulnerabilities, identify said vulnerabilities, and cross-reference them to the NIST CVE database. Although we did not discover any vulnerabilities I would be able to report any vulnerabilities effectively, and give a plan to respond to the vulnerabilities. My knowledge of the Wireshark tool allowed me to effectively scan for abnormalities in network traffic, and my previous courses would give me the knowledge to write an effective report on the abnormalities and pursue deeper investigation into abnormal traffic.

The phishing assessment task had me put into practice much of the same learned knowledge as the phishing simulation plan. However, I needed to provide a non-repeated example of a phishing attack. I learned that there were a multitude of different types of phishing attacks in university. I would have preferred to give a phone call example, or deepfake example given the new abundance of those types of phishing attempts. However, I decided to use a phishing example that used an official branding in a deceptive way, where the document access was the phishing link, rather than a traditional phishing link.

By far my most practiced skill from Old Dominion University is professional writing. In each of these assignments I had to do more than just perform a Cybersecurity task, I also had to write a report, plan, or response to the task. With all of my practice with professional writing, I was able to make effective reports, communication, and plans based on my previous knowledge of the assigned task. Additionally, my abundance of practice in researching for university had proved invaluable when creating both the phishing simulation, phishing assessment, and multifactor authentication plans.

Learning Outcomes

The four learning objectives I had for this internship were as follows: conduct effective penetration tests in a professional security environment, apply identity and access management controls, evaluate human-focused security risks, and communicate and document security initiatives clearly and concisely. I believe I accomplished each of these objectives at least partially.

I was able to conduct minor penetration tests within a professional security environment. I wanted to put to full use my knowledge of penetration testing, to conduct a sanctioned penetration test of the organization. However, that was not available, at the very least I was able to vulnerability scan, monitor network traffic, and learn WPScan. I do hope that I am able to conduct the phishing simulation by the end of this internship. I consider this a partial accomplishment, as I completed what I wanted on a much more surface level, and significantly smaller in scale.

Within the first few months of my internship I was able to identify potential identity and access controls issues regarding Google drive access. I wanted to develop a system to authorize and authenticate access based on role relevance and administrative oversight. I eventually was able to monitor access, but I was not able to conduct any authorization initiatives. The other relevant task to this was creating a multifactor authentication plan that outlined an initiative to enforce multifactor authentication for the entire organization. I would say this objective is partially accomplished because I was able to develop a plan, and theorize potential solutions to the authentication and authorization problem the organization faced. However, this plan has not gone into action nor have my team or I developed a multifactor authentication system that integrates with Striven properly.

Social engineering was one of the main security concerns of the organization when I first onboarded. Considering these concerns I was hoping to evaluate human-focused security risks. I wanted to develop a system that would identify potential vulnerabilities based on human error or social engineering. My first task related to this was the phishing simulation plan, which if put into action, would have logged and monitored successful phishing attempts on staff members and highlighted our weaknesses. The other task related to this learning objective was the phishing assessment. The phishing assessment provided a quiz to be taken by staff members that evaluated their security awareness around phishing attempts. This accomplishes my goal of evaluating human-focused security risks, and goes a step further by teaching test-takers about phishing attempts that are more obscure, and more effective.

My final objective to communicate and document security initiatives clearly and concisely was only partially accomplished. I wanted to be able to communicate security initiatives to non-Information Technology staff members, and ensure they understood what I was communicating. However, a majority of my communication was in the Information Technology department, and was rarely even cross-team. However I was able to communicate potential Cybersecurity initiatives to fellow team members and leadership. I was also able to create proper documentation procedures within the plans when the plans were to be implemented.

Overall I accomplished these learning objectives to a lesser degree than I had hoped. I wish to potentially further my accomplishment in these learning objectives towards the tail-end of my internship.

Emotional Aspects of The Internship

My first thoughts when receiving an internship offer from this organization was that of excitement and worry. I was excited to finally obtain an offer, especially so close to my graduation date. However, I was worried that I would be very unprepared for this internship, after all I had been applying and not been accepted by many previous internship opportunities. After seeing how rare an internship offer was for Cybersecurity, I was completely unaware of what to expect, especially from an organization that then onboarded me to a completely different organization from my original application. To note I was also uncomfortable working in a political campaign.

After general onboarding I was worried I wasn't as qualified as some of the other candidates and dealing with some imposter syndrome within the first week. However, after attending the first Cybersecurity meeting and receiving my first task, I realized that I was fairly well prepared for this internship. I was very excited at the prospects of conducting a phishing simulation and developing and integrating a proper multifactor authentication system that works with Striven. Leadership within the Information Technology and Cybersecurity departments were also interns, so I felt more comfortable communicating with them. Although much of the internship experience was not very well organized. For most of the internship I was excited to participate or lead some of the bigger projects. There were a few slumps where not much was going on, this was fairly discouraging. Especially the tail-end of the internship experience was discouraging, no Cybersecurity related tasks have been assigned, and I have only been assigned social media boosting tasks. It is incredibly disengaging to continue to do unrelated work to your internship specifications, but that is reasonable considering the rarity of a Cybersecurity internship at the time.

One of the most challenging parts of this internship was bridging communication between leadership, team members, and new onboarding interns. A lot of miscommunication and lack thereof was occurring when trying to get tasks ready for everyone, determine best suited based on skills, and ensure everyone was able to get experience within the internship. There were long gaps of no communication from leadership, and it was normal for a task to be assigned and there not be clarification until halfway to the expected deadline. I did my best to steer the team to be active and accomplish more when there were more tasks in the internship. I am very discouraged that I was unable to accomplish the large milestone tasks I had hoped to accomplish prior to my internship, although I didn't have that much choice in the matter. By far my biggest challenge was balancing time between my responsibilities as a full time student at Old Dominion University, part time employee, part time intern at another organization, and a part time intern at this organization.

Overall I was relatively excited with my internship. Over the course of the entire internship I would say that I am relatively satisfied with my experiences in the internship. Although I can only hope for more, I can only expect so much from an organization where Cybersecurity is not at the forefront of their concern. I am glad that I chose this internship to review over my other internship as this one was significantly more focused on uplifting interns to achieve their goals with the tools that they have within the organization. I'm not sure about the future of this organization, as its trajectory is heavily dependent on whether or not the organization founder wins election during this year's election in Florida.

Recommendations for Future Interns

There are a few things that I would recommend to future interns seeking internships at A Better Way Campaign. My first recommendation is not to fall for imposter syndrome, if you feel that you aren't as qualified as you'd like to be, there are plenty of people that can help you apply the skills you do know to the work you're assigned. Additionally there are plenty of departments that you can hop between where you think you would be best suited. My second recommendation is that communication is key. A majority of staff members are interns themselves, so communicating for clarification is necessary to being successful in your tasks. My third recommendation is to plan to do more than just Cybersecurity, a majority of my work has been Cybersecurity thus far, but the priority of the organization is to gain as much exposure for the founder as possible, so expect to contribute to that. My fourth recommendation is to learn to professionally write. A lot of your tasks will require you to abide by guidelines set by the department leads. Be concise and effective in your documentation. My fifth recommendation is to communicate a lot with your team. I found that the more I communicated and encouraged communication among team members, the more we would get done. My final recommendation is, if you are confident, seek a leadership role. I wasn't lucky enough to be accepted into a leadership role, but it didn't hurt to try. If you have the time and if you have the experience, a leadership role in your field will look better than if you didn't take that role. If you intend on getting an internship here, I wish you the best, and hope it meets your expectations.

Conclusion

In conclusion, this internship proved to be a valuable experience, even with the ups and downs. This internship allowed me to put into practice what I have learned in my Cybersecurity classes, and from my life experiences. One of the biggest takeaways from this internship was that it ended up being more about planning and documenting than applying technical skills from what I've learned. There were plans for bigger projects, and even if I don't see their implementation in my time here, I'll know that I created the first drafts, the structure of what it will be designed on. I was able to accomplish a lot of my learning objectives by the tail-end of the internship, I didn't accomplish them to the scale or quality that I had wished. Throughout the tasks in the internship I was able to apply many of the skills learned in university, with each task having a different application. The experience gained in collaborating and communicating with leadership, team members, and new onboardees, I learned a great deal on how to effectively communicate within these circles. Working in this internship has also shown me a lot of the challenges that leadership faces when prioritizing certain tasks, and what to do with a department that works better with already established infrastructure.

As I seek a career in Cybersecurity, I will apply much of what I have learned to future positions. Career experience and academic experience are two very different but incredibly important types of experience. I believe that I excelled in this internship because of my academic experiences, and my communication skills gathered from both university and my previous entry-level employment. I intend to incorporate my new knowledge of professional security environments, with the core knowledge of Cybersecurity and penetration testing that my academic career has provided. I intend on seeking for more applications of the curriculum I'm learning within my final semester at Old Dominion University. As I continue in my

Cybersecurity career, I hope to build upon my technical skills gained from my academic career, and the professional experience developed from my time at this internship.