CYBERSECURITY INTERNSHIP

Internship at The Global Electronics Association

CYSE368_24518
Spring - 2026
Teresa Duvall
Joshua Russell

Kyle Sershon – 4/15/2026

Table of Contents

Introduction

The Global Electronics Association is a non-profit that focuses on education, standardization and advocacy for the electronics manufacturing industry. Under the leadership of Chief Executive Officer John Mitchell and other executive staff, the organization has grown significantly and established a strong footprint in the industry. The organization offers education and certification for the electronics manufacturing workforce in addition to promoting workforce development through education outreach to public schools. Our standards team leads the charge in creating a baseline for the electronics manufacturing process, meeting with industry-leading committees around the globe on all aspects of manufacturing, including, but not limited to, packaging, wire harnesses, and printed circuit board design. Our government advocacy team works closely with the United States and other governments to advocate for material supply, clean and renewable manufacturing processes, and global industry partnerships.

During my education, I have found that specific skills cannot be learned solely through coursework and require practical experience to prepare for a career in cybersecurity. I have already spent close to a decade in the Information Technology field and currently hold the role of Infrastructure & Security Administrator. I have worked on a small team with the Global Electronics Association since February 2019. When I first started my position as a Level 1 Helpdesk Administrator, I had to quickly learn many skills that I did not obtain through my education in Information Systems at Oakton Community College.

One of the attractions of the organization to me was its focus on personal growth and family values, which aligned with my own values. I had the drive to succeed in building on a foundation laid while working toward my associate's degree in information systems. The Global Electronics Association, formerly IPC International, provided me with the experience I needed, which served as the brick-and-mortar foundation for building my career and knowledge in Information Technology. As the only helpdesk administrator for a staff of just under a hundred full-time employees, time management and task automation were essential to my role.

Reflecting on my earlier years, I quickly identified aspects of the information technology department that would benefit from a modern approach to the changing work environment. I quickly got to work scoping out improvement plans, such as adopting cloud device management for our mostly remote organization. I used foundational C++ knowledge to learn scripting and began automating tasks. This gave me more time to focus on improving our current operations, resulting in a more streamlined approach for both our staff and me. It didn't take long for my supervisors and leadership outside of our department to notice the value I brought. I always pitched ideas for improvement and took the initiative to learn new technologies and understand how they could benefit the organization.

After less than a year in the organization, I was thrust into my first cybersecurity incident. Our internal servers became infected with ransomware. The initial response was extremely stressful but required a calm, structured approach to mitigate the spread and isolate infected devices. The

process fascinated me, and I was eager to be involved in the remediation process and discovery. Ultimately, it was determined that the malware entered our systems via an infected email attachment sent to a user.

That brought my attention to the human behavior aspect of cybersecurity. Seeing how our own employees could be a threat due to social engineering and attackers' manipulation tactics piqued my curiosity. I also looked at my personal life. I saw family members become victims of scams, and observed threats during the COVID pandemic illuminated the true vulnerability of technology in our everyday lives. My son, in elementary school, started in a remote learning environment. I witnessed children falling victim to obscene “Zoom bombings” and the fragility of infrastructure in many networks, including that of our organization.

The personal curiosity I had about cybercrime, the real-world application of cyber defense in my everyday life, and the initiative to help improve our security posture at my employer led me to identify the need for cybersecurity expertise in our environment. I wanted to fill that role. I approached my supervisor with a goal, and leadership support was unanimous. After all, growth and education are core values at The Global Electronics Association.

As I progressed through my education and my role evolved, the opportunity arose to apply what I had learned full-time at our organization. The combination of my education and career experience puts me in a unique position to apply the foundation I learned at Old Dominion University to benefit our infrastructure. This provided me with the opportunity to intern as an Infrastructure & Security Administrator.

My objectives during my internship were

1. Apply cybersecurity principles and frameworks in a real-world enterprise environment.
2. Develop and implement security controls for identity, endpoint, and cloud-based systems
3. Analyze security risks, incidents, and system configurations to improve organizational security posture.
4. Demonstrate professional growth through documentation, reporting, and security awareness initiatives.

Because I had prior work experience in Information Technology, I did not have a formal training structure. I had weekly one-on-one meetings with my supervisor, Mark Campbell, to discuss new topics, such as network security in our environment. During these meetings, I received guidance and instruction based on the questions I brought to Mark about our environment. These meetings filled any gaps in my knowledge.

Management Structure

The Global Electronics Association has a hierarchical management structure. I directly report to my supervisor, Mark Campbell, whose official title is Director, IT Ops Systems & Infrastructure. Mark handles all aspects of IT ops, including but not limited to Dev environments, network infrastructure, and application environments. I work alongside Christopher Ramos, the Level 1 Security Administrator, who handles most of our in-house user service requests in the Jira ticketing system. Both Christopher and I report to Mark Campbell. Mark Campbell reports to Dave Ciaglo, who is the Senior Director of Enterprise Systems. Dave handles internal integration and planning for the organization's system development. Dave reports to our Chief Information Officer, Brent Laufenberg. Brent is an important part of our team and spearheads communication and planning between our executive team in each department. Brent directly reports to our CEO, John Mitchell.

I have found the management structure to be effective and to follow a more traditional format than one would expect in any organization. Our IT enterprise systems team, under Dave, is effectively separated from our development staff in our IT department. Though we assist each other, it allows our team to focus on the organization's operations. Our development team is also under Brent with a different Director. We can receive constructive feedback from other teams in the organization and, through Brent, communicate project feasibility effectively.

Major work duties, assignments

One of the first tasks I took part in was the remediation of our results from annual penetration testing. This year, our penetration testing tested both outside threats and insider risks. Overall, we received strong results, with only a few items identified as critical to fix. Among those, I focused on strengthening our organization's password policy. We changed our password length requirement from 7 to 14 characters. Additionally, we incorporated a list of “banned” passwords. This included any passwords that contained easily guessable phrases or characters like seasons, dates (ex: 2026 or Spring). This met the testers' requirements and strengthened the organization’s overall security posture.

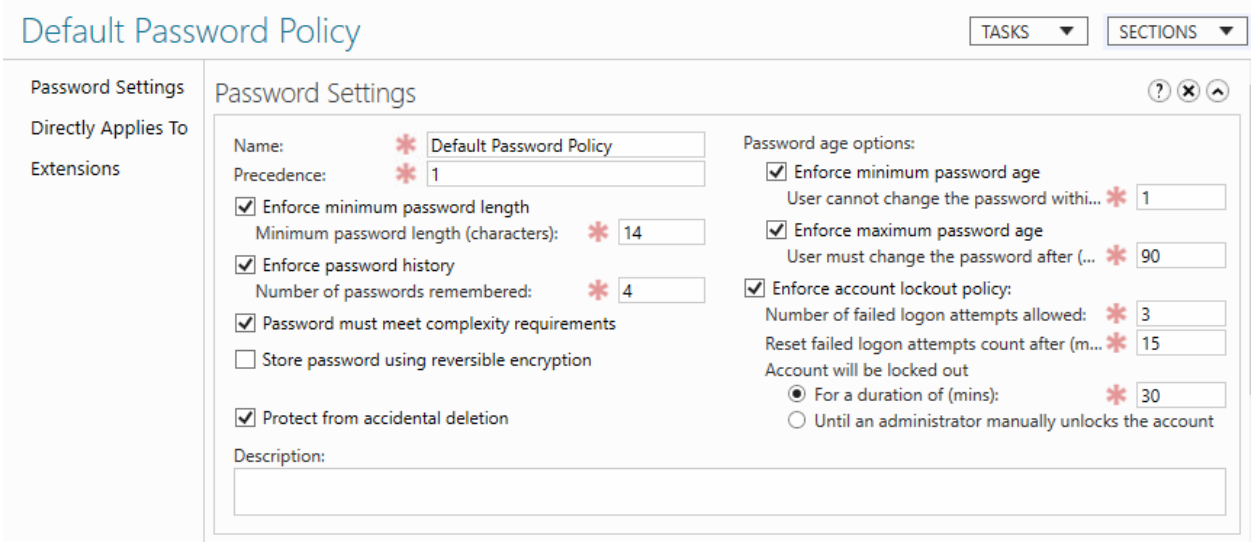


Figure 1: Default password policy for the domain – post remediation

In addition to a new password policy, I designed and led a quarterly phishing campaign to identify vulnerabilities with our staff. This gave me the opportunity to create remediation awareness training campaigns based on a user's "Risk Score" in the Knowbe4 Platform. As a result, the subsequent follow-up simulated phishing campaigns saw a reduction in failures by our organization's staff.

Simulated phishing campaigns are vital to any organization. Simulated phishing would be scheduled monthly, and the email format would be randomly generated using KnowBe4's templates. We selected Levels 1 and 2 from a 5-level scale, with 5 being the most difficult. It provides metrics on who has clicked links in emails, scanned QR codes, and opened attachments. It will also track when a user reports a phishing email. E-mails are tailored and customized to our organization's name, ensuring the user must carefully inspect each email to determine its validity. We typically choose categories related to multi-factor authentication and password expiration. This determines the user's risk score. Remedial training was issued to anyone who fell into a "Critical" category, and it was taken in tandem with our security awareness training campaigns, which are mandatory for staff.

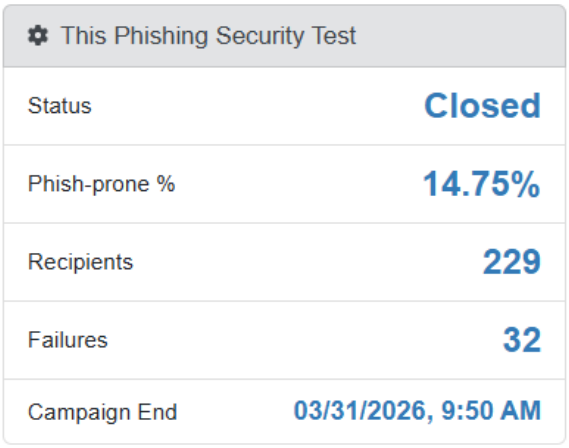
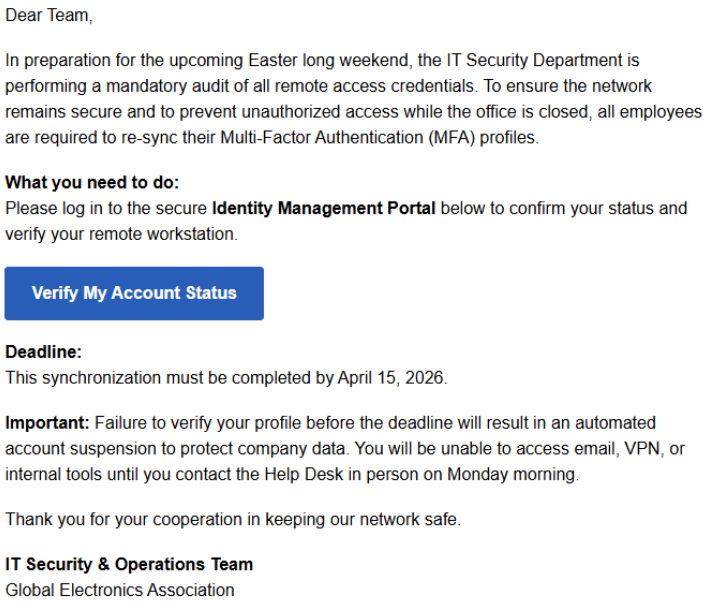


Figure 2: simulated phishing campaign results – March



Dear Team,

In preparation for the upcoming Easter long weekend, the IT Security Department is performing a mandatory audit of all remote access credentials. To ensure the network remains secure and to prevent unauthorized access while the office is closed, all employees are required to re-sync their Multi-Factor Authentication (MFA) profiles.

What you need to do:
Please log in to the secure **Identity Management Portal** below to confirm your status and verify your remote workstation.

Verify My Account Status

Deadline:
This synchronization must be completed by April 15, 2026.

Important: Failure to verify your profile before the deadline will result in an automated account suspension to protect company data. You will be unable to access email, VPN, or internal tools until you contact the Help Desk in person on Monday morning.

Thank you for your cooperation in keeping our network safe.

IT Security & Operations Team
Global Electronics Association

Figure 3: Simulated E-mail that resulted in a failure by a user

Our Security awareness training modules educate our staff on the latest attacks and methods used by individuals attempting to breach our network. The format is typically a 30- to 45-minute video, with questions in between to ensure the user remains engaged and understands the material. Through awareness training and phishing campaigns, we have been steadily reducing insider risk in our organization.

I worked closely with our backup infrastructure, exploring “Cold, Warm, and Hot” backups. It was important to consider the availability of these backups as I worked on the project to determine which model best suited organizational needs while balancing cost. Full backups were taken once a month, with incremental backups in between. My supervisor encouraged me to create a PowerShell script to automate the process. Since the task was routine and followed the

same structure each month, automating the monthly backups with a script ensures that backups are taken of our development servers and that email confirmation is sent for each job. It eliminates human error, ensures the integrity and availability of our information, and allows time to work on other tasks.

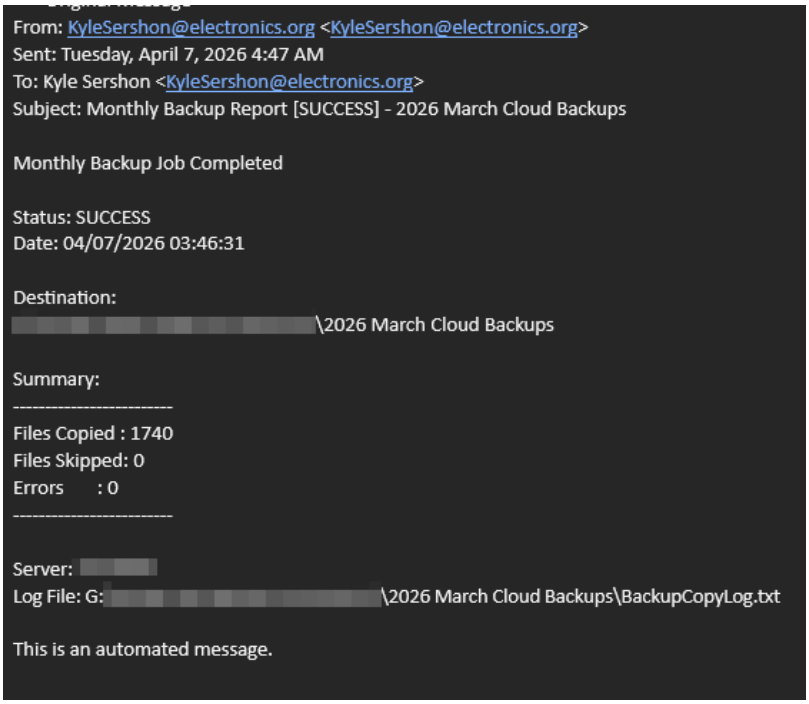


Figure 4: Automated E-mail for completion of backups

Though we store our Drupal backups locally, not all our backups follow this process. Using Veeam, we store our full server backups with a 7-year retention policy in an AWS S3 bucket in Glacier. Though retrieving information takes much longer in the event of loss, we reduce costs by storing our "Cold" backups here. Our development environment backups are stored for 1 year as ready "Warm" backups. This structure balances the best feasibility, cost, and availability. Scripting, in combination with the Veeam platform, ensures the integrity of our information.

Endpoint security is crucial to any organization, and continuous monitoring and investigation of potential malicious activity help keep it secure. Using CrowdStrike ESP for real-time scanning alerts the team to possible threats. During my internship, I monitored the alerts and responded to them as needed. This met my goal of analyzing and responding to incidents as well as reporting my remediation steps to my supervisor. Although we had no major concerns, we used this CrowdStrike information to identify a user who violated our Acceptable Use Policy. This occurred when "Roblox.exe" attempted to be downloaded and installed on the system. This action was blocked by CrowdStrike, and we reminded the user that, as part of our AUP, family members are not permitted to use company assets.

Though I worked on several smaller projects throughout my internship, my daily activities focused primarily on threat analysis and information security. I would spend time each day working on access controls to ensure users had access only to the information they needed. We

followed the principle of least privilege and a Zero Trust framework for our administrators and staff. Authentication was required for all access to information within our network, including for external users.

Skills

Before starting my internship at the Global Electronics Association, I had already worked in the Information Technology field for close to 9 years. I worked as a Level 1 and Level 2 Helpdesk administrator, gaining skills that I carried forward into my internship. I possessed an intermediate level understanding of the information technology field. One of the skills that benefited me throughout my academic career and that I brought from my profession is having a strong understanding of troubleshooting methodology. Additionally, I had a basic understanding of networking and information systems. I worked closely with Microsoft Cloud Platform and local servers. I had skills in Microsoft Server Manager, end-user support, and mobile device management, among other skills.

Prior to working in information technology, I was employed in the retail industry. Mainly working in customer service and management, with some experience in marketing. This taught me valuable skills that transitioned well into information technology. Soft skills, such as strong communication and empathy, were extremely beneficial early in my helpdesk role. I learned how to navigate corporate structure and hierarchy, as well as plan effectively to meet goals.

This combination of skills provided a strong foundation to build on once I transitioned to my internship. I used more advanced networking skills to help strengthen our overall security posture. Skills I learned regarding human behavior and computer crime allowed me to craft a training program for our organization to increase awareness. My knowledge gained in policies, standards, and compliance was applicable as I assisted my supervisors in documenting and drafting new policies for our staff, as well as in remediation during penetration testing. Overall, the skills I learned at ODU helped sharpen and refine much of what I already knew when I entered the program. I used this as an opportunity to fortify our defenses against threats we encounter every day.

Old Dominion Curriculum

I transferred to Old Dominion with an associate's degree in information systems and transferred a little over 60 credits. The rest of my degree was completed at Old Dominion. The curriculum at Old Dominion University prepared me for my internship in various ways. The program is interdisciplinary, drawing on several disciplines to achieve a comprehensive understanding of the subject. I focused heavily on the sociological aspect of cybersecurity throughout my educational journey. Given my real-world experiences and interests, I found that the area of cybercrime,

along with how technology affects society and the security concerns surrounding it, shaped my elective course choices.

Cyber Security Ethics, Cyber Law, and Cyber Security and the Social Sciences were all courses that gave me a foundational understanding of how to approach the world of cyber security. It provided the opportunity to critically think about how technology has changed and is currently evolving this world. Applying this to my internship, I can draw several specific instances in which this has helped me understand the challenges the field currently faces.

By combining an understanding of cybercrime with other social science-based courses, I gained insight into how threats impact our staff. Social Engineering is used by criminals to influence our users and persuade them to act on phishing emails. Using social engineering techniques, a criminal can tailor an email to a specific user, such as an organization's CEO. This is called whaling. Cybercrime is a multibillion-dollar industry, which underscores the strong motive for criminals to target organizations. By taking courses such as Cyber Security Strategy and Policy, I learned why organizations create policies based on the unique threats they face. The Global Electronics Association conducts business with government bodies worldwide. Working with multiple governments, our policy is designed not only to protect our information but also to segregate it to prevent unauthorized access.

Technical Courses like Linux System for Cyber Security, Digital Forensics, and Windows System Management and Security gave me foundational technical knowledge on how systems work together and how to implement a strong security posture across them. Delving into specifics, I learned how an attacker can manipulate and exploit these systems to gain unauthorized access. Understanding how an attacker might gain entry enables us to focus on and harden the areas most easily exploited.

Using those principles during my internship, I could apply what I learned to help segregate information, focus on access to specific areas of information for our users, and help enforce and implement strong policies that strengthen our standing. Basic networking and programming helped me understand how computers ‘think’, allowing me the opportunity to create effective scripts and benefit from a strong troubleshooting methodology when approaching tasks.

Outcomes for objectives

Above, I listed the objectives I had during my internship. My internship effectively fulfilled each of my goals.

1. Apply cybersecurity principles and frameworks in a real-world enterprise environment.

   To achieve this objective, I applied cybersecurity principles to our enterprise environment. My assistance with the Penetration test remediation gave me the opportunity to fully understand the requirements and apply knowledge from the

curriculum. Additionally, my work on the company's backup infrastructure gave me the opportunity to apply to the CIA Triad. I was also able to apply my understanding of "The human factor," cybercrime, and social engineering to implement a phishing campaign and security awareness training.

2. Develop and implement security controls for identity, endpoint, and cloud-based systems.

   To achieve this objective, I directly worked with the organization's password policy in Windows Server Manager and implemented a stronger policy to reduce the risk of brute-force attacks. In addition, I spent time using the Microsoft 365 administration center to refine conditional access and Intune MDM policies. Using role-based access control (RBAC), I worked with some of our staff to grant limited editing access to SharePoint and to limit access for the helpdesk team.

3. Analyze security risks, incidents, and system configurations to improve organizational security posture.

   During my internship, I achieved this objective by analyzing CrowdStrike system detections. Resolving "Risky" user detections in Microsoft Entra was also a regular task. This gave me the opportunity to analyze and remediate risks with both endpoints and user accounts.

4. Demonstrate professional growth through documentation, reporting, and security awareness initiatives.

   By documenting each incident and all the tasks I completed, I met this requirement. I demonstrated growth during my internship by directly applying what I learned from Old Dominion University's curriculum to each objective I completed.

Motivation and Challenges

One of the most motivating aspects of my internship was the opportunity to work directly in a cybersecurity-focused role. I was able to apply the knowledge I gained in my coursework directly to an organization I have been affiliated with for years. Strengthening systems and applications in our environment, knowing I was constructing a strong posture for our staff and team, was a major driving force. One of the primary motivations for pursuing my degree in Cyber Security is understanding the threats our enterprise and people face every day. Not only in my professional life, but also in my personal life. Helping protect my grandparents and parents from scams and understanding the risks my son and the younger generation face growing up in a

constantly online world gave me the most motivation. My strong desire to help others motivated me highly during my internship.

Although my internship offered many valuable learning opportunities, I realized that not every challenge could be avoided. Even after setting up strong phishing campaigns and training, we still had a relatively high failure rate. Though this may have been mildly discouraging, I was able to reframe this as an opportunity to identify what other systems I could strengthen to fill the gaps. Scripting was also discouraging at some points. Spending several hours working on a script, for it to continually fail during testing as I refined it, was a laborious task. Though the trade-off of constructing a functional script and presenting a strong solution and product could often help overcome that discouragement.

The challenges I faced were the sheer magnitude of the systems involved. I realized quickly that I had to prioritize tasks and create proper documentation to stay on par. This, unfortunately, would mean some tasks lower in priority could not be completed. During my internship, organization was key to success. Additionally, asking for help when I needed it was important, and I found that my supervisor appreciated it. Though I had a strong desire to showcase my skills, I needed to approach each challenge with an open mind and realize that it was okay to ask for help when I didn't fully understand a particular objective.

Recommendations

The world of Cybersecurity requires a diverse number of skills to succeed, but the most critical skills are not something you can learn out of a textbook. There are soft skills you can practice developing that will take you far in a Cybersecurity internship. For instance, strong communication, the ability to listen to your coworkers and supervisors, is important. Don't be afraid to ask questions as you learn a new role as well. Approach those outside of the technical field who come to you for help with empathy and understanding. These are all important soft skills to possess, which will help you excel in an internship.

For technical skills, I recommend learning to script in bash or PowerShell. Automating repetitive tasks can help free up your time to work on other issues. Make sure to thoroughly document all processes and changes while you work on any project. Before starting your internship, try to understand the scope of your work and the systems you will be working on. Brushing up on those specific systems before you start your internship can help give you an important edge.

Conclusion

The field of cybersecurity is complex and does not encompass only one field of study. This applies both during education and while fulfilling a professional role. Cybersecurity as a profession requires a unique set of hard and soft skills to succeed. During my internship, I gained

valuable practical knowledge of how cybersecurity impacts every aspect of an enterprise. Without cybersecurity playing its critical role, an organization or business could easily become a target, leading to reputational damage and severe financial losses.

During my internship, I was able to apply many technical skills every day, which helped to build upon the foundation of my educational path. It was very enlightening to see how cybersecurity operates within an enterprise Information Technology Department and how it is the lifeblood of any organization. The vast array of systems and technologies used made it clear I could never be an expert on everything, leaving my path going forward full of diverse choices.

As I continue my education, even into a master's program, I see that many businesses and organizations are heavily using Artificial Intelligence across every part of their operations. With this new technology comes its own set of challenges, such as proper use, information protection, and Intellectual property. Artificial Intelligence is a powerful tool that can also be used by those who wish to exploit an organization's systems. If I were to continue into a master’s program at Old Dominion University, I would like to learn as much as I can about security around artificial intelligence to keep up with modern enterprise environments.

As I continue to move forward in my career, my internship has strengthened my desire to dive deeper into preventing cybercrime wherever my journey takes me. Reflecting on my internship, I found the most valuable aspect to be the satisfaction of preventing another attack and the stress it has on both enterprise systems and their staff. My internship has emphasized to me just how important education is for staff. The need to stay vigilant and alert will always continue as I move forward in my career.

Cybersecurity has proven to be a meaningful career with many paths forward. My internship has given me the opportunity to understand the inner workings of an enterprise networked system. I enjoyed identifying and researching applications and policies to ensure they met our organization's needs while optimizing costs and security. The opportunity to help and educate others while protecting our assets made my internship meaningful. I found that using the education I received, coupled with my previous work and life experiences, maximized the benefit I gained from an internship in Cyber Security. I look forward to continuing my career in Cyber Security and pursuing further education to help others.