Internship Report: IT Help Desk and Cybersecurity Experience at Plasser American

Jacob Carney

Old Dominion University

CYSE368/Internship

Professor Teresa Duvall/TA Joshua Russell

04/19/2026

Table of Contents

Introduction

Plasser American is a multinational manufacturing and engineering company that deals with the services and equipment for maintaining railroad tracks. The company belongs to a larger global network and has earned a good reputation due to decades of innovations in railway technology. Its key products are track tamping machines, ballast regulators, and rail inspection systems, maintenance, and technical support services that provide the safety and efficiency of the rail infrastructure. The organization mainly caters to freight rail, passenger rail, and government transportation agencies that depend on accurate equipment to build, inspect, and maintain tracks. I decided to intern at Plasser American as it provided a chance to get hands-on experience of working in an enterprise IT setting and enhance my expertise in cybersecurity and technical support. The size of the company and its dependence on secure digital systems offered a perfect environment to see the IT service management in action. The main areas I needed to achieve are my troubleshooting skills, understanding of cybersecurity measures, including identity management and secure access controls in line with the principles of Zero Trust (Rose et al., 2020), and becoming a competent communicator in assisting non-technical users. This internship provided a good rapport between theory and practice in cybersecurity operations in a professional business setting.

My internship started with a series of orientations, which taught me about the organization of the IT department, support processes, and security expectations that govern the day-to-day operations. I was taught how to use the Jira ticketing system, how to escalate, and how to interact with end users in a professional manner. The first thought that came to my mind about the company was that it has a very organized and professional working environment with a high focus on efficiency and cybersecurity awareness, which stimulated my interest in the field. This paper summarizes my internship experience, including my learning goals, training, and career development in the company. The intertwining of modern technologies and engineering that the company has undertaken underscores the significance of safe and effective IT procedures in assisting massive industrial operations.

Management Environment at the Internship

Organizational IT Structure and Management Framework

The IT department at Plasser American has a hierarchical system of management that is based on the tiered support model, which aims to streamline efficient management of technical problems and stability of systems. At the foundation is the help desk team, where I worked as an IT Desktop Support Specialist. Senior technicians, system administrators, and IT managers are above this position, and they are in charge of infrastructure, cybersecurity policy, and enterprise systems. This stratified system enabled the provision of clear routes of escalation and effective allocation of duties. The company also coordinates its IT services with current security governance practices, such as identity governance and access control models that make sure that the users can access systems relevant to their jobs only (Glockler et al., 2023). This hierarchy

formed a well-defined chain of command that minimized the levels of confusion and enhanced accountability of day-to-day activities.

Supervision and Leadership Style

The practice in the internship was supportive, organized, and very practical, particularly in the initial phases of my training. Mentors such as my immediate supervisors and senior technicians offered me constant mentoring by shadowing, inspecting the tickets, and involving me in the process of troubleshooting. The feedback was often instantaneous, and I was able to rectify the errors and improve on my technical style quickly. Leadership style focused on mentorship and not on strict control, which promoted learning and independence as time went by. This solution is in line with the principles of experiential learning in teaching cybersecurity when practical training increases skills retention and professional preparedness (Bertone et al., 2025). As I continued, my supervision became less direct as time went on, with the supervisor making less frequent check-in visits, increasing trust in my skills, and allowing me to find my own solutions to IT problems.

Communication, Ticketing System, and Workflow Efficiency

One of the key elements of management performance was the application of the Jira ticketing system that organized the way tasks were assigned, tracked, and closed. A ticket would have all the documentation of what the user had said was wrong, how urgent it was, and how to fix it. Supervisors tracked the flow of tickets to make sure that service-level expectations were achieved, and high-priority incidents were escalated accordingly. This system enhanced accountability and transparency in the IT department. New studies have pointed out that specifically IT service management systems, with an additional feature of AI-based support tools, can be of great benefit in the efficiency of response and workflow (Malla, 2026). In my case, Jira also fulfilled the same purpose as it minimized the number of miscommunications and provided an opportunity to all team members to access real-time updates about the issues at hand.

Cybersecurity Governance and Management Practices

Cybersecurity awareness and governance were also a major concern in the management environment. The management of identity and access-controlled security policies, which controlled employee authorization and organizational adherence policies.This can be compared to the cybersecurity framework in the enterprise, which aims at safe authentication and role-based access control to limit risk exposure (Glockler et al., 2023). Further, the values that were followed within the organization were similar to the idea of Zero Trust Architecture, within which no user or device is presumed to be trusted even within the internal networks (Rose et al., 2020). The supervisors always enforced safe behaviors, like password checking, multi-factor authentication, and sensitive data handling. Another critical security issue identified is human factors involved in thwarting social engineering attacks, which are considered to be the biggest cybersecurity threat in organizations to date (Tan et al., 2025).

Major Work Duties, Assignments, and Projects

Overview of Core Internship Responsibilities

My main roles during the internship at Plasser American as a Desktop Support Specialist under the IT department involved offering technical assistance to end users, managing IT systems, and ensuring seamless day-in, day-out operations of the enterprise technology services. I was organized around the help desk resolution of tickets, system troubleshooting, user accounts, hardware and software support, and performing routine IT maintenance work. Such duties played a critical role in ensuring continuity of operations within departments since employees strongly depend on functional technology in order to deliver their duties effectively. Studies have indicated that proper management of IT services is essential within contemporary organizations since it directly determines productivity, security, and organizational performance (Malla, 2026).

Help Desk Ticketing and Incident Management

Working in the Jira ticketing system to log user issues, track, and resolve them was one of my most common tasks. A ticket had to be documented with proper attention to the problem, troubleshooting measures taken, and the final solution. I dealt with cases like login issues, bugs, problems with printers, and network connectivity problems. Effective ticket management was critical to ensuring transparency in the workflow and proper escalation of unresolved issues. This also assisted in creating a knowledge base applicable to the recurrence of technical issues. Alexander and Wang (2024) found that in IT systems, structured data collection enhances cybersecurity monitoring and allows organizations to respond to incidents more effectively because it allows them to identify patterns in system malfunctions and user problems.

User Account Management and Identity Administration

The other significant responsibility was in handling user accounts using Active Directory. This involved the password reset, unlocking of accounts, assigning permissions, and onboarding of new employees into relevant system groups. These activities were important in ensuring security in access control in the organization. A major part of enterprise cybersecurity includes identity management, since this way there is always a risk of unauthorized access; it is also important to provide users with only the systems related to their work (Glockler et al., 2023). My efforts in this regard helped to facilitate operational effectiveness and alignment with cybersecurity, so that the employees had an opportunity to use the required tools without undermining the organizational security policies.

Hardware and Software Support

I also assisted hands-on with hardware and software troubleshooting, such as desktop computers, laptop computers, docking stations, monitors, printers, and network troubleshooting. This included troubleshooting physical connections, driver updating, reinstallation, and faulty equipment replacement, where possible. Also, I helped in the implementation of new systems, installing Windows-based operating systems, and setting up vital company applications. These activities were needed so that the workers would have safe and sound workstations. The study of cybersecurity has highlighted the importance of having well-configured endpoints that decrease their vulnerabilities to ensure that the entire organization is well-positioned in countering cyberattacks (Afolalu & Tsoeu, 2025).

System Maintenance and IT Support Tasks

My tasks also included performing routine maintenance. These consisted of installing software updates, system checks, and preparing devices for new employees. I also facilitated keeping secure settings on company devices, ensuring that IT policies are adhered to. These activities are significant as old-fashioned systems tend to be more susceptible to cyber assaults and malfunctions. According to cybersecurity research, regular system updates and maintenance would greatly decrease the vulnerability to existing vulnerabilities and enhance the resilience of the organization (Cremer et al., 2022). Engagement in these activities helped to ensure that the IT environment was stable and secure.

Use of Cybersecurity Skills and Knowledge in the Internship

Pre-Internship Cybersecurity Knowledge and Foundational Skills

Before starting my internship at Plasser American, I received the majority of my knowledge of cybersecurity in the classroom setting and by way of theory. I was taught about basics, such as confidentiality, integrity, and availability (CIA triad), and the principles of network security, authentication, and risk management. I also got a slight introduction to identity and access management concepts, malware types, and basic security measures, such as password hygiene and multi-factor authentication. To a large extent, much of this knowledge was theoretical and not practical. According to Zwelling et al. (2022), cybersecurity awareness is not a successful practice, as the real-life environment teaches that the behavior should be flexible and requires making decisions that are practical to cope with threats in the most suitable way.

Application of Cybersecurity Practices in Daily Tasks

During my internship, I was able to apply some of the most important principles of cybersecurity in a few real-world scenarios, namely user account management, incident handling, and system access control. One of my main duties was to handle user identities with the help of Active Directory, which demanded to implement secure authentication policies and to be able to assign permissions appropriately. It was a straight translation of the identity and access management (IAM) concepts that are top priority in limiting unauthorized access in enterprise environments (Glockler et al., 2023). I also did not involve myself in the verification process, before changing the passwords or unlocking the accounts, and this again added momentum to the necessity of undergoing an identity check-up as a safety measure and to prevent any attempt of unauthorized access.

Cybersecurity Skills Learned on the Job

Although I went into the internship already possessing a base of knowledge, I acquired a lot of new skills in the process of the hands-on experience. Among the top skills that I acquired is hands-on incident response in a help desk setting. I got to know that I should evaluate the seriousness of problems, prioritize tickets according to the risk and business impact, and escalate the issues when needed. The process enabled me to learn how cybersecurity incidents are dealt with on a real-time basis in organizations. I also got to know how to be aware of possible security risks when performing regular IT support. As an example, in the course of troubleshooting user devices, I felt a greater awareness of suspicious logins, out-of-date software vulnerabilities, and poorly configured systems. Research shows that human perception and immediate identification of abnormalities in IT systems are essential in attaining cybersecurity performance (Tan et al., 2025). The experience helped me to understand the importance of frontline IT support personnel in the defense of cybersecurity in organizations.

Shift in Understanding of Cybersecurity Concepts

My practical experience as an on-the-job learner greatly altered my thinking about cybersecurity, as it helped to switch my point of view from theory-based knowledge to a practical one. My pre-internship perspective of cybersecurity was that it was a technical area that dealt with firewalls, encryption, and antivirus programs. Nonetheless, the experience of working in the actual IT environment has shown that the issue of cybersecurity has all to do with human behavior, communication, and organizational processes. I gained a better idea of how human factors lead to security risks. To illustrate, I noticed that user errors, including the use of weak passwords or inefficient use of login credentials, could expose weaknesses. Human behavior is one of the greatest causes of cybersecurity attacks (Tan et al., 2025). On the whole, my internship has enabled me to combine academic theory of cybersecurity with the practical experience of real-world IT support. I also did hands-on tests in identity management, incident response, and safe system maintenance, and solidified the things I studied at school.

How the ODU Curriculum Prepared Me for the Internship

Academic Preparation and Foundational Knowledge from ODU

Old Dominion University (ODU) course offered a solid theoretical basis that helped me adapt to the real world of an IT help desk setting at Plasser American. The cybersecurity basics, networking, and IT systems courses made me learn the basics of network architecture, authentication systems, and the foundations of cybersecurity, including confidentiality, integrity, and availability. These introductory subjects played a critical role the first time I encountered the work with enterprise systems and troubleshooting technical problems. Studies focus on the importance of cybersecurity education in higher education to equip students with the skills to deal with real-life threat scenarios. However, it is typically necessary to complement it with more practical knowledge (Siphambili, 2024).

Connections Between Classroom Learning and Internship Tasks

My internship experience allowed me to make some direct correlations between what I studied at ODU and my day-to-day tasks. As an example, the concepts that I learned in identity and access management classes were directly applied when I was working with Active Directory to manage user accounts, reset passwords, and grant permissions. These assignments were practical demonstrations of the principles of access control under real-life conditions, which I had already learned in theory. In the same vein, networking coursework assisted me in learning about connectivity issues, IP settings, and which steps to undertake to troubleshoot network-related situations. Furthermore, the layered security and secure authentication frameworks that we talked about in the classroom gained relevance when I could see them in work practice in an enterprise setting. My internship experience was especially pertinent to the Zero Trust security model that presupposes that all users or devices should not be considered trusted by default (Rose et al., 2020).

Areas Where ODU Prepared Me Effectively

ODU equipped me with the necessary level of technical thinking, problem-solving strategies, and awareness of cybersecurity. Structured troubleshooting methodology was, by far, one of the most useful skills I gained at school, which I utilized when working on the help desk support. This involved the typification of issues, variable isolation, solution testing, and

recording of findings. These were steps that were very much aligned with the actual IT support processes. Cybersecurity awareness was another well-prepared area. The courses focused on the necessity of secure behavior, recognition of risks, and data protection measures. This was in line with studies that indicate that awareness and behavior of cybersecurity are essential factors in thwarting security incidents (Zwilling et al., 2022). I applied this knowledge during my internship when working with sensitive data, when helping users with their authentication problems, and when identifying the possible security risks of the system's work.

Areas Where the Curriculum Was Limited

Even though ODU offered a good theoretical basis, certain areas of the internship had some drawbacks that showed a lack of practical training. A significant weakness was the inability to be exposed to actual enterprise tools like Jira, Active Directory, and large IT service management systems. Although I was familiar with the principles of IT service workflows, my practical experience and use of these tools in the real world had to be learned and adapted on the job. Moreover, the unpredictable user behavior and time pressures of real-world troubleshooting were not always well-known in simulated situations in the classroom. Studies emphasize that experiential learning would also be crucial in cybersecurity education as it helps overcome a gap between what students learn in theory and what they can put into practice (Bertone et al., 2025).

New Skills and Concepts Learned During the Internship

The internship has introduced me to some of the new concepts that I had not been able to discuss in my coursework. Among the most notable ones was the operational framework of the IT service management within a corporate setting. I was able to learn how ticket prioritization, escalation process, and workflow management directly influence organizational efficiency. I also acquired some hands-on experience in cybersecurity risk detection from the perspective of support, especially in detecting initial symptoms of system vulnerabilities or security risks associated with users. Also, I got to know why human factors play a role in cybersecurity, particularly the role of human behavior in posing security threats like the use of weak passwords or poor usage of systems. According Tan et al. (2025), the human aspect continues to be among the greatest problems in managing cybersecurity.

Evaluation of Internship Outcomes and Objectives

Overview of Internship Objectives

In the introduction to this paper, I have already listed three key learning outcomes of my internship in Plasser American: (1) to deepen my expertise in troubleshooting and technical support in a real enterprise setting, (2) to sharpen my knowledge about cybersecurity practices, particularly, identity/access management and (3) to improve my professional communication skills in my interactions with both technical and non-technical users. All in all, these goals informed my internship experience. They supported the way I organized my learning outcomes in meaningful ways in accordance with the expectations of the industry of IT support and cybersecurity.

Objective 1: Strengthening Troubleshooting and Technical Skills

The first goal was met completely with the help of regular practical work on practical IT problems. During the internship, I was engaged in troubleshooting hardware failures, software

errors, network connectivity issues, and system-configuration projects. The structured troubleshooting strategies assisted me in gaining better diagnostic reasoning and problem-solving skills. Experience-based learning is the most effective in enhancing technical competence in any cyber and IT setting (Bertone et al., 2025). Throughout my internship, my technical confidence and efficiency significantly grew as I was now able to solve most of the typical problems and escalate complicated ones more efficiently.

Objective 2: Understanding Cybersecurity Practices and IAM

The second goal was to learn more about cybersecurity practices, specifically identity and access management. This was also achieved by using Active Directory to manage user accounts daily, reset passwords, and give assignments on permissions. These activities directly echoed the principles of identity governance, which are fundamental to the security of enterprises (Glockler et al., 2023). I also had practical exposure to security policies like authentication checking and the access control process. Also, I gained awareness of cybersecurity threats, such as human factors vulnerabilities, such as poor passwords, and social engineering threats. As it is stressed in research, human behavior is a key determinant of cybersecurity effectiveness (Tan et al., 2025), which became even more prominent in my real-life experience.

Objective 3: Improving Professional Communication Skills

The third goal was to sharpen the communication skills in the technical support setup. In part, this goal was met and, at the same time, kept developing during the internship. The ability to use email and phone as well as face-to-face communication with users helped me feel more comfortable talking to users, especially making technical problems sound like a simple explanation. Nevertheless, I also learned that IT support communication needs to be constantly enhanced, especially when it comes to dealing with frustrated clients and making complex technical issues easy to understand. User communication and awareness play a crucial role in effective cybersecurity and IT support (Zwilling et al., 2022). In general, my internship at Plasser American has effectively achieved all three learning objectives, although there are still things to be improved. The goals connected with technical and cybersecurity-related elements were highly met through the way of working practice, and communication skills were developed gradually, but could use further practice.

Most Motivating and Exciting Aspects of the Internship

Exposure to Real-World IT Problem Solving

The best experience of my internship at Plasser American was that I got an opportunity to apply technical solutions to real-life contexts of an enterprise. In contrast to the classroom activities, where the situation is simulated and has a predictable outcome, the internship opened me to unpredictable and time-sensitive problems like system failure, failure to log in, and hardware failures. Every ticket closed made me feel like achieving something since I realized that my work helped directly to facilitate employee productivity. This educational interaction supported the importance of experiential learning, which is a necessity when it comes to the development of professional competence in cybersecurity and IT careers (Bertone et al., 2025).

Hands-On Cybersecurity and Identity Management Work

The other factor that was very encouraging was being able to work directly on identity and access management systems by working on the Active Directory. Such activities as password resetting, unlocking accounts, and user permissions made me feel like I had contributed to the cybersecurity posture of the organization. Of particular interest to me was learning how access control systems are used to secure sensitive company information by ensuring that only authorized users gain access to particular resources. The studies highlight that identity and access management are significant aspects of enterprise cybersecurity as they minimize the risks of unauthorized access and enhance the integrity of systems (Glockler et al., 2023). My involvement in this process helped me to make the cybersecurity concepts I learned in school a reality and make it a powerful concept.

Developing Independence and Confidence

Towards the end of the internship, I felt more independent in dealing with tickets and solving technical problems without being supervised. This increasing independence was very encouraging as it showed confidence in my supervisors and my rising ability. I also started to discern the patterns in the common IT issues and implement solutions more effectively. This correlates with the results, which suggest that learning environments, based on experience, can positively affect confidence and decision-making in technical sciences (Siphambili, 2024). The more autonoetic I had become, the more I was motivated to take the initiative and to enhance my performance.

Team Collaboration and Knowledge Sharing

Another interesting experience of the internship was working with the IT team. This also led to knowledge sharing as the collaborative environment facilitated the technicians to assist one another in solving complex problems. This collaboration helped to complete problematic tasks more easily and gave me a chance to observe the work of seasoned specialists. Studies indicate that teamwork and mutual understanding are necessary in enhancing the effectiveness of cybersecurity and organizational resilience (Zwilling et al., 2022). My position in a team of encouraging and efficient IT team members encouraged me to constantly develop my skills and remain involved in the learning process.

Overall Motivation and Career Inspiration

All in all, the best part of the internship experience was the glimpse of how cybersecurity, IT support, and problem-solving combine in a real organization. This experience reinforced my desire to work in the IT and cybersecurity field because I was able to see the practical effect of these jobs. It also rejuvenated my drive to keep on acquiring technical and professional skills that are critical in the current digital work environment (Tan et al., 2025).

Most Discouraging Aspects of the Internship

Initial Learning Curve and Technical Overwhelm

The most depressing experience about my internship at Plasser American is the steep learning curve at the beginning of the training process. Even though I already had the knowledge (based on my coursework), when I first entered a real enterprise IT environment, it was overwhelming. A considerable change had to be made to learn to navigate the Jira ticketing system, comprehend internal IT processes, and adapt to a fast-paced flow of support requests.

Sometimes, I experienced pressure in my attempt to find solutions fast and at the same time maintain accuracy. This experience is similar to research on cybersecurity education that finds that many entry-level professionals have difficulties transitioning between the theoretical approach to learning and real-life practice because of insufficient hands-on exposure (Siphambili, 2024).

Handling High-Pressure and Time-Sensitive Issues

The other demotivating factor was the urgent technical problems when time was running out. There were those tickets that needed urgent handling as they influenced employee productivity or access to the system. During such moments, the need to solve problems within a short time and not to commit any errors was difficult. In some cases, several problems were being reported simultaneously, necessitating prioritization and working with several tasks simultaneously. Although these experiences contributed to the development of resilience, they were initially stressful and at times discouraging. Studies on IT service management show that workload and prioritization of incidents are possible factors that can add stress in help desk settings, particularly among entry-level professionals (Malla, 2026).

Communication Challenges with Non-Technical Users

Sometimes communicating with non-technical users was also discouraging, particularly when the user had lost his temper or just could not comprehend the troubleshooting instructions. There were instances where a company had to re-explain things in order to assist the user in following directions, which prolonged the resolution time and pressure. This demonstrated the significance of communication in IT support jobs. Human factors and communication barriers are a major issue in cybersecurity and IT settings that can easily impact efficiency and incident resolution (Tan et al., 2025). These exchanges were frustrating at times, especially when the users were tense or lost.

Repetitive Nature of Certain Tasks

The repetition of certain tasks of the help desk, including password reset, account unlock, and simple troubleshooting, was another discouraging factor of the internship. Although these functions are necessary in running the organization, they were repetitive at times and were thus considered monotonous. However, I also learned that such activities are significant in ensuring that there is productivity and security in the organization. Studies highlight the importance of routine IT support functions as a keystone to cybersecurity operations despite being possibly repetitive (Afolalu & Tsoeu, 2025). Notwithstanding these disappointing factors, I realized that they were a significant element of my career development. These difficulties assisted me in becoming resilient, patient, and flexible in an actual IT setting. Gradually, I gained confidence to deal with pressure, communicate with users, and perform repetitive duties in an effective manner.

Most Challenging Aspects of the Internship

Complexity of Real-Time Troubleshooting

Among the hardest ones during my internship at Plasser American was the area of troubleshooting in a live enterprise setting in real time. In contrast to the classroom activities where problems are simplified and designed, real-life IT problems were usually complex, unpredictable, and demanded fast decision-making. There were numerous cases where several

potential causes were considered, which included software conflicts, network problems, or human errors, which complicated the diagnosis. I was forced to understand how to effectively isolate issues in a systematic manner and reduce the downtime of end users. This is consistent with studies that show the reality of IT support contexts is that they demand a high level of analytical skills and systematic problem-solving methods to effectively deal with complex interactions with systems (Malla, 2026).

Balancing Speed and Accuracy Under Pressure

The other significant difficulty was the speed versus accuracy of the process of solving support tickets. Lots of problems needed to be solved as soon as possible because they affected business activity, which put pressure on solving these problems swiftly. Nevertheless, haste in solutions occasionally adds to the risk of errors, particularly when dealing with sensitive tasks, like user accounts or the configuration of systems. This dilemma may be compared with the field of research in cybersecurity operations, which states that incident response must be efficient and precise to prevent the further introduction of vulnerabilities (Cremer et al., 2022).

Understanding Enterprise-Level Systems and Security Protocols

Implementation of systems like Active Directory, Jira, and internal security policies at the enterprise level was also difficult to adapt to. These systems had to be very procedure-oriented and able to pay close attention to detail, particularly when dealing with user permissions or troubleshooting access problems. It has required learning and experience to understand the mode of operation of identity and access management systems in a large organization. Studies emphasize that online systems of identity governance are challenging yet necessary to sustain security and manage access in enterprise setups (Glockler et al., 2023). These systems meant that one needed to adapt and be attentive to detail continuously. All in all, the complexity of real-life IT settings, the stress to be effective, and the necessity to master enterprise tools and cybersecurity processes were the most demanding parts of the internship.

Recommendations for Future Interns

Technical Preparation Before the Internship

The future interns who will join the IT Desktop Support job position at Plasser American will need to work towards developing solid knowledge bases of basic IT systems before they are engaged in the internship. This involves knowledge of operating systems (particularly Windows environments), fundamental networking concepts, and troubleshooting processes. It would be particularly useful to be familiar with such tools as Active Directory, ticketing systems, and remote desktop support platforms. Students who have had hands-on experiences in cybersecurity and IT internships before entering these programs adapt faster and work more efficiently in enterprise settings (Bertone et al., 2025). A strong technical base minimizes the initial learning curve and enables the interns to be more confident in making contributions.

Cybersecurity Awareness and Best Practices

Enhancing cybersecurity awareness, especially regarding identity and access management, passwords, and social engineering threat recognition, should also be part of the preparation of interns. It is important to know how secure systems are practiced within the enterprise environment. The learning in cybersecurity highlights that human factors contribute to

security breaches the most, and human awareness training is crucial to all IT staff (Tan et al., 2025). By knowing these risks upfront, intern students will be in a better position to observe the security regulations and safeguard confidential data in their day-to-day activities.

Communication and Customer Service Skills

Effective communication abilities are also needed to excel in this internship. The future interns need to be ready to explain the technical problems in a simple manner that can be understood by non-technical users, and be patient with frustrated people. In IT support environments, effective communication enhances user satisfaction and decreases response time. Studies have shown that the effectiveness of cybersecurity and IT support is not only based on technical expertise but also on how well they communicate effectively with end users (Zwilling et al., 2022). Professional communication is an important aspect that practicing prior to beginning the internship can help to enhance performance.

Professional Readiness and Work Habits

Interns must also have good organization and time management skills. The help desk situation is rushed, and various tickets need to be prioritized. Discipline, attention to detail, and being a proactive person will assist the interns in dealing with the workload. Moreover, it can be beneficial to comprehend the working processes of IT service management to be ready to operate in a formal setting based on ticket tracking and escalation protocols (Malla, 2026). In general, the technical and soft skills preparation will guarantee a more successful and easier internship experience.

Conclusion

The Plasser American internship was an extensive learning experience that enhanced my technical, professional, and problem-solving skills within a real-world IT support setting. During the experience, I had hands-on exposure to the practice of troubleshooting, cybersecurity, identity management, and enterprise IT operations. The lesson about the application of classroom knowledge to practical job duties, particularly in the fast-paced help desk environment, was one of the most valuable lessons. I also got to know that communication, patience, and attention to detail are important factors that should be considered when working with users who have different levels of technical skills. Altogether, the internship assisted me in becoming more confident regarding my abilities and understanding the cooperation of IT and cybersecurity in terms of supporting the efficiency and security of organizations. In the future, this internship will play a strong role in my upcoming life at Old Dominion University, as well as my future career in IT and cybersecurity. It has enabled me to know what I need to work more on in areas of troubleshooting, enterprise systems, and communication during crises, which will determine my future coursework. I will use these lessons in more advanced laboratory and practice settings in cybersecurity to enhance my technical capabilities and practical work. I will also utilize this experience to follow my career path to IT support and cybersecurity positions to add to my technical and professional skills earned during the internship and ensure my ultimate success in the IT field in the future.

References

Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges, and solutions. *Future Internet*, *17*(12), 575–575. https://doi.org/10.3390/fi17120575

Alexander, C. A., & Wang, L. (2024). Cybersecurity data sources and practices. *Journal of Computer Networks, 12*(1), 1–6. https://www.sciepub.com/portal/downloads?doi=10.12691/jcn-12-1-1&filename=jcn-12-1-1.pdf

Bertone, B., Wagner, P., & Pauli, J. (2025). Experiential learning: Innovative approaches to post-secondary cybersecurity education. *Journal of Cybersecurity Education, Research and Practice*, *2025*(1). https://www.researchgate.net/publication/395499103_Experiential_Learning_Innovative_Approaches_to_Post-Secondary_Cybersecurity_Education

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering*, *66*. https://www.researchgate.net/publication/373868826_A_Systematic_Review_of_Identity_and_Access_Management_Requirements_in_Enterprises_and_Potential_Contributions_of_Self-Sovereign_Identity

Malla, P. (2026). Improving IT support efficiency through an AI-Powered ITSM Chatbot. *International Journal of Artificial Intelligence & Robotics*, https://www.researchgate.net/publication/400216567_Improving_IT_Support_Efficiency_through_an_AI-Powered_ITSM_Chatbot

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST SP 800-207). https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Siphambili, N. (2024). Exploring cybersecurity implications in higher education. *European Conference on Cyber Warfare and Security*, *23*(1), 526–531. https://www.researchgate.net/publication/381651668_Exploring_Cybersecurity_Implications_in_Higher_Education

Tan, D., Rafsanjani, A. S., Aslam, S., & Behjati. (2025). Human factors in information security: A quantitative study with technical solutions to prevent social engineering attacks. *Digital Threats Research and Practice*. https://www.researchgate.net/publication/395432425_Human_Factors_in_Information_Security_A_Quantitative_Study_with_Technical_Solutions_to_Prevent_Social_Engineering_Attacks

Zwilling, M., Klien, G., Lesjak, D., et al. (2022). Cyber security awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://www.researchgate.net/publication/339273589_Cyber_Security_Awareness_Knowledge_and_Behavior_A_Comparative_Study