Integrated Video Solutions, LLC

Davon Mason

CYSE 368 Fall 2022

Table of Contents

Having to have an internship after being in the military was the most humbling thing that I've have done in recent years but at the same time it has helped me tremendously. Coming into the internship my expectations were very low because I was thinking that all the experience that I had gained over the years would be thrown out the window because I was in school but to my surprise, I was given a chance to prove myself. My experience was more of a manager's position, so this allowed me to grow in my career because I was only a journeyman in telecommunications, and I was unable to really understand the decisions and coordination it took to complete a project. Some of the objectives I wanted to receive from this was to become experiencing working on the civilian side in cybersecurity and open more opportunities for me in my career to thrive at the top level.

I decided to do my internship at Integrated Video Solutions, LLC because I wanted to experience how working outside of the military as a civilian would be as a network professional. This gave me the opportunity to experience how the knowledge I gained could be implemented in real world scenarios like managing a team of technicians, coordinating plans of implementation with other companies, and understanding more of how business is handled between projects and contracts. In this paper I will be sharing my experience in this internship from when I started to present time. Some of the information that will be shared will be vague due to sensitive information and policies that I must abide by, but it should still be understandable.

Integrated Video Solutions, LLC is a local minority and V3 Certified small business. Integrated Video Solutions, LLC, began sub-contracting to the Government on May 16, 2005. Integrated Video Solutions, LLC, works with commercial, state, DoD, and local government entities that extend a multitude of services supporting ship repair, electrical, telecommunication, navigation, data security, and other supporting services under DoD, NAVSEA, ISO, and NIST standards and policies. As an Essential company, IVS started by providing services for installing and supporting custom video display walls and CCTV for commercial and military needs. It has then grown to shift the focus to add more services in cybersecurity and network communications. This was a key role during the beginning of the pandemic for companies shifting to more of a remote networking infrastructure for its users. Along with supporting the company installation of network equipment IVS added more services that were tailored to adding components for personal protective equipment devices, extending the focus of how innovative the business is becoming.

My initial impressions of the position were based off word of mouth because I knew one of the workers in the company. They gave me some insight into what he was looking for and what it was he wanted to do in the future. In my mind I was wondering if I would be a good candidate for the position because in was currently in school and I also had other responsibilities that could possibly put me in a difficult position on choosing to focus on finishing school or leaving school and focus on the job. I wasn't sure if I could keep up with job tasks because my last job was a more controlled environment, and most issues were fixed within the community of the military. Since I had contacted my advisor about how internships worked at Old Dominion, I was more comfortable with meeting him to get to know who he is and what his business was about. In my initial orientation was very relaxing and ensuring that he was more of making sure he knew the goals and personalities of his employees. Some of the things we discussed were based on my experience, schooling, and goals for the future. My background in networking and communications from my past job allowed me to understand and can install and configure network devices. I was qualified in making coax, ethernet, and fiber cabling from repairing to troubleshooting, along with skills in radio and satellite communication.

Since I was in the military, I had already known the policies and steps to take when dealing with their devices and policies. As was engaged in conversation I was able to explain my job in the military and how I wanted to do more so I chose to leave the military to enroll in school to receive my degree. We then began a conversation about the degree I was seeking and what I wanted to do when I finished. At the time I was stuck between penetration testing and cybersecurity architect, he asked if I wanted to work for as part time to update his network and make it more compliant for government and DoD agencies, so I agreed. The management environment is like a small community of likeminded individuals with the same goals in line with the prosperity of the business and teamwork.

The management team of around five to six people that incorporate multiple positions, the president oversees the contracts between agencies and coordinates with the others on the management team to create plans, objectives, and manpower of what terms needs to be met. He prepared project updates, billing, reports, proofreads, and reviews the accuracy of all outgoing documentation and correspondence. He oversees employee training, workers' compensation, general liability, payroll, clearances, and staff certifications, and maintains all employee records and training records. He serves as the company's E-Verify Administrator and arranges all clearances processed to be completed for business purposes. The vise president deals more with the day-to-day task of the job. He's the person that oversees the manpower and physical task being completed for the contracts like training, skillset selection, and daily operations. When it comes to equipment usage, project management, and quality assurance is the person in charge. Then there is the security manager that is responsible for clearances, trainings, certifications, background checks, and other information that is responsible for secure measures for the business and external entities. They create, execute, and monitor the office security policies, procedures, and practices in compliance with Government security requirements. Ensure COMSEC requirements and procedures are being implemented and followed while providing guidance and instructions to all employees to ensure any event, circumstance, or acts that could be considered a breach of security. Maintain office records in compliance with our security manual and COMSEC procedures and ensure employee clearances are current, initiate non-access shipyard badges requests and background checks, confirm employee information via E-Verify, inform cleared personnel on their security responsibilities, safeguard company and employee information and comply with the National Industrial Security Program. With the security manager I work extremely closely with their department because of the information that is shared between both parties.

The Technicians in the business were the ones that did the work on the ships and other locations. Most of the job consists of installing, maintaining, repairing, and modifying different types of radar, radio, and phone systems alone with internet services. They were responsible for audio, visuals, and security systems including electronic connections. They had to be responsible for HAZMAT and OSHA standards along with other standards they had to abide by. For my job position I was responsible for ensuring and delegating a world-class customer experience to all our end-users while leading a department of IT professionals and supporters to a designated pool of our customers day to day task and IT needs, with a multi-functional skillset in IT resources, spanning from Level 1 to Level 3. As Lead System Administrator I function as the hands-on IT manager and expert for all computer systems and devices for local and external users. For this role I relayed on my strong technical background coupled with leadership skills that embrace a culture of employee growth and development coupled with a desire to deliver a world-class computing experience to all end-users based on the teaching and foundations installed in from the military. Specific use of knowledge of cybersecurity in the internship was very vital because I was responsible for all information security. To start I was responsible for assessing the current network to make sure then previous network was up to standards with different frameworks and DoD regulations. There were many meetings and webinars that I had to be a part of because I needed the information and the know-how to implement the required security measures. Knowing skills like cable management, system security, network configuration, firewall and other software knowledge allowed me to be trusted with correcting and installing the security measures. Knowing encryption is a skill that I feel is the most important skill to have at this position because of how much information is being transmitted through emails. Also knowing the types of vulnerabilities and malware used by attackers as another big plus because when the network was being configures, we were getting a lot of phishing attacks and ransomware because the email server that was being used was compromised. By knowing the severity of the issue, I was able to secure information that was not affected by creating a new email server with better security.

The on-the-job experience allowed me to see information security in the real word is so important because before I started this job, I didn’t expect that small business would be attacked for their information compared to larger corporation that have more information and resources. What I was told was that because we are a small business the figure that the security would be easier to compromise due to limited resources and that since they are affiliated with larger companies it can be easier for hackers to infiltrate by using the smaller company as a cover and a trick to gain access to the lager company information. The information that they use for smaller business includes information like contacts, address, and account information so they can target people or create fake websites or emails that are tailored and targeted to specific positions or employees.

ODU cybersecurity program prepares me for many of the tasks that I was involved with, allowing me to be the expert at my position and field of study. Most of the classes that I had taken in ODU worked hand and hand with issues that had came up from knowing how to make straight-thru ethernet cables and explaining the differences between the cable speeds to selecting the right server to install for the business. For example, CS-464, IT-315 and CYSE-270 helped me understand how to build a network infostructure from the ground up. It allowed me to make changes to the current network system and update the network with justification on why specific devices were needed. When I was task with this, I had the information to enforce the importance of having updated computers were a need and not just something that was seen a just a tool while also explaining how unsecure it was to have programs for unreputable sources could cause harder ache in the long run. This led to the president of the business and I examining network devices that would benefit the business by creating budget, security, and training plans. I even implemented tools that I learned for ODU to monitor the network to further protect the system checking a large portion of multiple assessment checklist needed to continue operating existing contract and acquire new ones at the same time. Classes CYSE-280, CYSE-407 and CYSE-450 helped me create protocols for the network servers and policies for the users of the network. These classes allowed me to understand the correct programs and tools for the business needs like when explaining that we need a server to store information in a single location instead of having information on multiple computers, the classes allowed me to explain the differences between clients, server, and give them details between what specific server does and how it can improve the functionality of workflow in the office.

The internship fulfilled experience working on the civilian side in cybersecurity. It gave me more insurance on what was required for a position and gave me the opportunity to figure issues out without having stipulation on the tools or requirements needed to complete tasks or troubleshoot. I was able to put my knowledge to the test and create a product that I can one hundred percent say that I did, it gave me confidence and a feeling of appreciation because I had created something by myself and made the company performance increase. It gave me credibility that I do have a grasp on what it is to be cybersecurity professional, and I have the skills to prove what I can do.

This internship opened more opportunities because I was able to network with other that work in the same career field as I and they were able to see the work that I can do along with my personality and focus. I have met a lot of professionals and company owners that are interested in me to ether work for them or to work with them in setting up or monitoring equipment for their business because of how well I was able to make an impact of the company that I currently intern at. As I push forward for my career, I feel that if I keep doing what I need to do while investing in my education in and out of school I can be a valuable commodity in this community.

What I found the most exciting aspects of the internship was the ability to work by myself instead of having large groups of people checking in and adding input on my job tasks. It allowed me to be in the zone when I was connecting equipment and building the infrastructure. This allowed me to finish tasks in a timely manner while having to not stress about finishing assessments in school or worrying that thing not being completed or rushed resulting in mistake or causing larger issues to arrive. I was able to plan and execute my ideals fire the network system and experiment with what would work or if some of the equipment could be abandoned that was either taking up space or was out of date.

The most discouraging thing for me was when I had to figure out the issue with encryption and email certificates to be accepted for government emails and communication the issues to the boss and contacts. A lot the pressure fell on me because in my mind the issue had to be fixed and with all the information that I could gather, they wouldn't be able to send information. I thought I may have messed up in some part of the update or if it would be something I could fix by myself, but I was relieved to find that what I had done was correct. I was the other party's issue that needed to be, so we corrected by using other was to bypass some of the measures until the issue was resolves. The most challenging aspect of the internship was making sure that I was holding my weight in the company and not slowing down production but to maintain it or improve. With the pace of things being slower than what I was used to it gave me a lot of down time that could have been used for anything, instead I tried to make use for my down time to understand the needs of the business for the future and ways I could help the business with the goals they had. Things like preparing the business for its next move to a larger location, I made sure that all the devices like phones, printers, and security cameras were POE so they wouldn't have to worry about purchasing new equipment but instead they could just add more to the switch if need be. I created documents that would keep track of tools and equipment so nothing could be lost or stolen. Little things that I saw I could improve on are the things o focused on to stay busy and show that I was not just here to receive a grade, but I was here to help in any way I could.

My recommendations for future interns arriving for this internship would be to come prepared to work and learn on the job. Be ready to use the information that you learned in class and apply it to the tasks given to you and don't think that you know everything. Another big thing that I learned quick is to listen to what is going on and to others' ideas. When you come into the internship be prepared to feel that everything you learned in school is not the same as it is in work. The theory behind what is going on in the job is the same thing the only difference is that most tools and equipment that is being used may be outdated or it can be something that may have been only used for this specific company. I would also recommend that they be prepared to do multiple task that may not apply to what you want to do in cybersecurity like you may have a task to work on programing radars or planning out the best location for placement of device to work proficiently and be them most effective. Don't say that you know how to do something if you really don't know how the skillset, even if you may have learned about it but not physically done the task because it can be very difficult from what you may have seen on websites or in school. In all for new inters applying for work it is best to be respectful to all the employees that work there no matter the position they hold and be motivated with doing every task that s handed to you because most the time I feel they are trying to see what they can trust you with and if they can trust that you are a asset, you have a better chance of having a permanent position in the business.

What I got from this internship was confidence and the ability to network within the community. The internship allowed for me to experience what it is like to manage to small group of techs and balance timing and task. I was able to be a leader and allowed my team to be more efficient on the job with tricks I learned from prior experience and classes in school. I gained trust and respect from my peers at the business, and it made the moral of the job higher and allowed me to be accepted as a qualified worker. Making contacts and working relations with the other company officials and professionals educating me on business aspects on cybersecurity like job positions that are need and job outlooks in the area. They gave me information about what programs to signup for that would help my career along with what things in need to do to tailor my resume for the exact position I want.

This internship gave me prospective to what part in cybersecurity I wanted to focus on in my career path. It allowed me to narrow my choices down to a couple of positions that I would have never thought about or knew that existed. I feel more equipped and ready for the future in cybersecurity, and I can't wait to start my new chapter in my life.