Internship Reflection Final Paper

# Caleb Mayo

# Employer: Library of Virginia

# Course: CYSE 368

# Term: Summer 2023

# Table of Contents

Page 1 – Introduction and Learning Objectives

Page 2 – Brief History of the Organization

Page 3 – First Day at Internship and Management Environment

Pages 4 & 5 – Internship Duties

Page 6 – Skills

Page 7 – Outcomes Fulfilled and ODU Comparison

Page 8 – Motivations, Discouragements, Challenges, and Recommendations

Page 9 – Conclusion and Link to E-Portfolio

# Introduction

I decided to attend an Internship at the Library of Virginia because of two reasons. One of those reasons was my lack of acceptances from more technical internships with organizations that had a focus on Cybersecurity. My GPA was unfortunately not up to par with other applicants, however my experience in previous opportunities such as working as an IT Systems Support Technician at Costar along with my two Industry Professional Certifications, the CompTIA A+ and CompTIA Security+, gave me a good foundation to land the interview with the Library of Virginia. Not only that, but this Internship was close to home, in the city of Richmond Virginia, so it would be the perfect commute compared to a previous position offered by Apex Systems, which would have me commuting to Virginia Beach. I had caught wind of the LVA Information Security Intern position by looking at Federal Job sites and consistent searching.

## Learning Outcome #1:

One learning outcome I hoped to achieve from working as an Information Security Intern at the Library of Virginia is how to operate at a state agency level. Since a vast number of jobs and opportunities in the Cybersecurity Field are in the Public Sector with government agencies, I would need to know how they operate and see what pros and cons there are to working within a state agency compared to working in the Private Sector with small businesses, corporations, and Fortune 500 companies.

## Learning Outcome #2:

Another learning outcome I looked forward to from my time at the Library of Virginia was technical experience. Since gaining my two CompTIA certifications, my main goal has been to gain more technical experience and work on more projects in cybersecurity. And in the interview with my supervisor before they offered me the intern position, she explained that I would be working alongside the Information Technology and Risk Management Teams at the Library of Virginia. On top of that, any experience working with an organization can provide me with useful information and skills that I can apply to any future opportunities out there for me after this internship.

## Learning Outcome #3:

Learning more and attaining more professional development is a great learning outcome I expect from the Library of Virginia. The itinerary for the Internship had multiple events where interns could meet and converse with different departments at the Library of Virginia about their experiences and some insight into how to propel our careers.

# Beginning of my Internship

# Brief History of LVA

As previously mentioned, for the Summer of 2023, I interned at the Library of Virginia in Richmond, VA. The library was founded by the Virginia General Assembly in 1823 and was meant to be a collection of books and documents important to Virginia’s history since the founding of the Colonies. Over what is now an outstanding 200 years of growth, the Library of Virginia has become not only a collection of Virginia’s books and documents, but a hub for the history of Virginia’s citizens and their contributions to the world. The library holds an enormous collection of data in the form of print, manuscript, photographs and digital collections. The library also works as a consultant to state officials for Virginia history and uses it data to create resources such as publishing some of its own award-winning books on Virginia History, providing Federal and State Grants, and its amazing Exhibitions, lectures, and book-signing to communicate Virginia’s vast history and culture to the public. As a matter of fact, one of LVA’s new projects, “Virginia Untold” is diving into the untold stories and history of Virginia’s enslaved and African American community and culture.

# First Day at my Internship

My first day at LVA had me surprisingly very anxious as I was unsure what to expect. When I had walked into orientation, and everyone introduced themselves. I had come to realize that I was the only intern directed towards IT or Information Security. My fellow interns were assigned to other departments in the library, such as Digital Collections and Processing. We were given a tour of LVA and all of its facilities, as well as shown some of the cool Exhibitions and documents that the Library had. One of my favorites that we saw was a against a County of Virginia that ended in an enslaved person and their family gaining their freedom which was over 100 years old. Later on, we had our pictures taken for our ID badges, which we use to navigate the building, and we then went our separate ways with our supervisors. My supervisor let me know that my internship would be different from my fellow interns, as they would be working primarily on Library Projects, while my supervisor would assign me some weekly tasks that would help educate and build my skills in Information Security. I then met the Information Technology team and all of the interns and supervisors reconvened for an intern lunch. Another aspect of my internship I was surprised to hear was that most of my work and duties would be done remotely, and I had the option to work from home for a majority of my internship. My initial impressions of this internship after my first day was that it was going to be a fun experience, and would have me involved in a lot of projects that I wouldn’t have normally expected myself to be in. The workplace environment was super friendly and knowing that I wasn’t the only intern that would be working at LVA helped with my anxiety quite a bit. Getting to know them as well, even finding out one of them was attending Old Dominion University’s online program next Fall was interesting.

## Management Environment

The management environment for my internship was a lot more laid back than I expected. For nearly all of my tasks that my supervisor assigned me, which is upwards of ten or twelve assignments, she has only actually touched base with me about two of them. There has not been a lot of communication between her and myself, but she does try her best to include me on upcoming projects with the LVA and working with staff on software such as the new SIEM that the Information Technology team implemented. However, any time I had an issue or trouble understanding one of my tasks, she was easily accessible and ready to communicate the objective to me effectively and efficiently.

# Internship Duties

Many of my internship duties are completely unnecessary to how LVA runs things. As my supervisor described it to me, she would give me a multitude of tasks to do that would not exactly be used to help LVA, but would give me knowledge and experience in certain areas of Information Security. Even before my tasks were assigned, my supervisor asked me the main things that I wanted to learn or get more experience on from working at LVA, so that implied to me that she didn’t really have a plan for me to help with anything at LVA. The very first task that she assigned to me was to read all of LVA’s Information Security Polices and Regulations and briefly summarize them on a word document. This task helped me understand how auditing and policy compliance worked for state agency as well as helped me develop my policy-reading skills. The standards that LVA follows are from the Virginia IT Agency’s website and are readily available to be followed and adhered to by the commonwealth. The next task that she had me do was study networking and create my very own network diagram. This part was especially challenging because she wanted me to create a specific type of network diagram that she did not convey very well. After I created one with the simple devices and network layout, she told me to redesign it to be more “robust” and “detailed”. After a solid couple of hours of frustration and confusion, I had to ask her to elaborate a bit more, in which she showed me a version of a network diagram that was much more complicated than the one I had developed, but I had a solid vision of the outcome she wanted. In the end, I created a meticulous network diagram with all the needed applications, software, and ports listed as well as the security measures taken to secure it in a small description. I think this task was probably my most beneficial because it taught me a little bit more about networking that I didn’t know about before I started this internship, and it also taught me to not give up when I am frustrated and to put my ego aside and ask for help because executing someone’s vision is more important than getting it right the first time. The next task that I did was practice my auditing skills with the new Security Incident and Event Management (SIEM) software known as Log (360). I even worked with a couple other members of the IT Team in setting up alerts for possible security events happening on the network by running scripts. The only two downsides to this task were that I had to do a lot of reading of the Information Security Standards to understand what alerts to set and the fact that I had little oversight for this task. It was a great learning experience as I learned how to create scripts for alerts based on what the Information Security Standards needed. For example if the Information Security Standards needed me to have a limited number of login attempts for a user, I would set an alert that would notify me or the system administrator when someone reached that number of login attempts. My Week 4 Assignment had me studying and researching Application Security and Security Monitoring. The task was to identify and fix security vulnerabilities within a simple web application. This task had no specific web application my supervisor wanted me to work on, so I verified with her that I could use one of my own and after getting the okay, I worked on one of the modules on the Cybersecurity Learning website known as TryHackMe. This task was definitely my easiest one. For Week 5, one of my most proud assignments, I was tasked with creating an Access Control Policy for 5 divisions or a large company that have interconnecting missions. This task was hard for me because I didn’t exactly know what divisions to do or how I should organize the access control policy. It took a lot of research and comparing other access control policies to create my own, and I had to understand the requirements that each division needed for access control. In the end, it was quite a task and I felt successful in achieving it. On week 6, I developed a training presentation for the staff of the Library of Virginia to highlight the key points on the Information Security Policy. I used PowerPoint to create it and added slides from each part of the Policy explaining what this meant for the staff and how they should use it in their days working at LVA. The slides contained pictures and actual real-world scenarios in how the Information Security Policy was implemented. This would have been exciting to present to the staff, but I was never scheduled to. For Week 7, I was tasked with analyzing and evaluating the security of a Cloud Service Provider. I chose Amazon Web Services (AWS) as my CSP because I was already studying to pass the Amazon Certified Cloud Practitioner Certification Exam. With AWS’ many Cloud Instances, I decided to research the cloud security of their most common instance, the Amazon Elastic Cloud 2 (EC2). Then, I proceeded to research their many whitepapers on its security as well as its features and uses. I found in my studies of it that EC2 is heavily secured and has a two part Shared-Responsibility Model where the client or user running the Instance secures the front end of its group policies, network policies, and access controls itself, and Amazon secures the backend features as in everything that keeps the instance running. For Week 7, I designed an Incident Response Plan for a Virginia State Archive. The hardest part about creating this Incident Response Plan was tailoring it towards a Virginia State Archive, which can hold many valuable assets such as digital archived Documents as well as physical historical documents. The best way I thought to execute this was to follow the format of an Incident Response Plan from the NIST cybersecurity framework. I created sections based on each step in the framework: Preparation, Detection and Analysis, Containment and Eradication, Post-Incident Activity and Recovery. These sections would highlight the steps and standard procedure for the Incident Response Team to take when a problem concerning Information Security, whether it be a DDOS attack or something as simple as a natural disaster took place. At the time of me writing this paper, because my internship is ongoing until Early August, my supervisor has me working on a case-study of my choosing, and I am also working on a showcase of my learning and experience at the internship, which I will present on the last day of it. As I stated before, I don’t believe that any of my work was necessary or essential to the duties and mission of the Library of Virginia, other than a measure of the experience and work environment from me.

# Skills and Knowledge Used During Internship

Easily my most used skill during my internship at LVA in terms of Cybersecurity was my ability to research. Since all but one of my assignments had been without supervision from my supervisor, I had to learn much of the information needed to complete these assignments by researching them myself. This is a great skill that will continue to help me in Cybersecurity, mostly because it is an ever-changing environment. Learning within this internship has taught me that everything needs cybersecurity, and to give the best cybersecurity possible, you need to cater to your assets needs, strengths, and limitations.

# Comparison to ODU Curriculum

The ODU Curriculum from my experience has a broader take on Cybersecurity as the courses I’ve taken have broader applications to the public and private sectors compared to the cybersecurity of a Library. However, the Library of Virginia is still a state agency and ODU’s curriculum accommodates for this through one of its major required courses, CYSE 250. I got a good general understanding of how to see Cybersecurity in nearly every aspect of life.

# Were my Expected Outcomes Fulfilled?

## Learning Outcome #1

I can genuinely say that learning how to operate at a state agency level has been a well fulfilled learning outcome from me working at LVA. Compared to working at a private organization such as Costar, there were a lot more regulations in the policy that had to be considered for a state agency. Working in teams was different as well as there was a bit more leniency when working for a state agency I felt. Overall, it was a great experience and I had fun every day I came in-office with the IT Team.

## Learning Outcome #2

My technical experience has gone up in areas of Cybersecurity I didn’t think I would see progress in. I gained some good insight into using the Log360 SIEM Software as well as the auditing process. Even though these skills aren’t always thought of as technical skills, they are essential to proper cybersecurity.

## Learning Outcome #3

My professional development has gained some decent connections in my time at the Library of Virginia. By going to scheduled-intern events as well as spending time working on projects with my peers on the IT Team, I have gained two business cards and connected with 5 other employees on LinkedIn. Not only that, but knowing that my experience at LVA is going to support my resume exponentially is a good feeling.

# Motivations

The most motivating aspect of the internship was the experience. Being able to say that I can not only function but think critically and work well in a state agency environment was a good motivator. Another aspect of it was that I was motivated to not stop there. I didn’t want to be just a member of the IT Team, for my career I am envisioning and working towards a leadership position in executing someone else’s vision.

# Discouragements

The only way I really felt discouraged was in how this wasn’t like a traditional internship, or that’s how I perceived it. I didn’t feel generally integral or valued on the team as much as I thought I was, and the lack of supervisor involvement didn’t help that.

# Challenges

The hardest part about working at LVA as an Information Security Intern was learning to ask for help when I needed it as well as finding the best way to research for my assignments. Both were mitigated as soon as I asked for help, and thus was able to achieve the task better when I knew what outcome was needed.

# Recommendations?

In my opinion and based on my time at LVA, I would recommend this Internship for any rising Cybersecurity major. It gives you a good chance to do your own research, as well as work in a Public Sector. Not only that, but the hours are quite flexible, and if you engage in opportunities when they come, you can learn a lot at the Library of Virginia.

# Conclusion

The Library of Virginia is a great place for your first internship. I developed my skills in Research, Auditing, and Project Work which will all make me a better in my Cybersecurity career. This internship also taught me that sometimes the first step is not always what you think its going to be. I thought I would be more hands on but I was a more passive intern and watched how the LVA operates and can bring the skills I was taught to my next organization as well as my ODU campus. This internship has made me a better student and better person as I will be more open in the future.

E-Portfolio Page Here