Capstone Reflection: Anthem Blue Cross Blue Shield

Jesse Chin

CYSE 368

Fall2023

**Table of Contents**

**Introduction………………………………………………………………………………………1**

**Content**

History…………………………………………………………………………………….1 Orientation & Training…………………………………………………………………....2 Initial Impression………………………………………………………………………….2

 Management Environment………………………………………………………………...3

 Duties & Responsibilities…………………………………………………………………4

 Figure 1…………………………………………………………………….4

 Figure 1-2………………………………………………………………….4

 Skill Set……………………………………………………………………………………5

 Curriculum Comparation………………………………………………………………….5

 Meeting Objectives………………………………………………………………………..6

 Internship Aspects & Preparations………………………………………………………...7

**Conclusion………………………………………………………………………………………..8**

This past semester, I enrolled within the CYSE 368 course with the purpose of experiencing an internship and completing my degree in cybersecurity at Old Dominion University. That being said, my experience may have differed compared to other students due to the fact that I was approved to use my full-time job as a substitution for a traditional internship environment so long as aspects of my job involved topics of cybersecurity and IT. The reason I chose to work for this company was simple, I needed a paycheck. However, the reason why I decided to utilize my current position as my internship was because I believed it would be able to provide a unique perspective that I wouldn’t normally be able to get as an intern working from a technology-based team and/or position. The memorandum had asked that we as students provide a list of learning objectives we wished to acknowledge and focus on during our time at the internship. My learning objectives I believe were direct and simple: to gain a better understanding of the industry, to have a better understanding of the cybersecurity laws and policies at which my company is forced to uphold (mainly HIPAA laws), to build a better understanding of information technology and cybersecurity needs in a non-standard environment (such as the sales department), and to see if I could get more exposure to traditional cybersecurity topics and concepts within a corporate setting such as: incident response and recovery procedures, practical applications with access control, cybersecurity awareness training, etc. As the paper continues, I further explain whether I was able to meet my learning objectives, whether aspects had changed, and my overall experience in changing perspectives from working as an employee to someone who is focusing on the technology and cybersecurity needs from a day-to-day basis.

 Before I delve into the details of my experience, it is important to understand some facts about the company I work for. I am employed under Anthem Blue Cross Blue Shield, an American health insurance carrier that exists and provides coverage across multiple states under various subsidiaries and branches. The company was founded in the 1940s under the name Wellpoint but is known by other names and branding depending on what state the coverage is in: Empire Blue Cross Blue Shield, Horizon Blue Cross Blue Shield, Care First Blue Cross Blue Shield, and so on. Most recently, the company has rebranded under the name Elevance Health, but will continue to be referred to as Anthem within the rest of the paper as that was the name during my hiring process as well as being its most well-known branding. Anthem is a Fortune 500 company that provides all forms of medical insurance including: dental, vision, life, disability, and assists with coverages in Medicare and Medicaid and have been listed as part of the top 10 healthcare companies from the Forbes Fortune 500 yearly listings. Because of the wide range of health coverages available and the country’s continuous need for healthcare, Anthem doesn’t have a select demographic they cater towards. All products are made available and target to all manners of people regardless of gender, age, ethnicity, etc. They sell their coverage to both large corporations and small, private businesses as well as making their products available to those who have a need for individual policies, Medicare, and Medicaid.

 I was initially hired four years ago into the company under a different position, broker services, which mainly dealt with assisting clients and was recommended to my current position as an Account Coordinator by the hiring manager later-on. The job posting for this title could only be hired internally as there were several mixed requirements and skills that were recommended for the position. There wasn’t truly anything note-worthy during my orientation aside from understanding the physical security measures implemented at the home office where I worked. All new hires had their picture taken, and printed onto ID badges which are required to always be on hand while on company grounds. The badges act as digital security keys that are required to be scanned in order to be granted access to the office, but of course certain restrictions are in place preventing individuals from having unauthorized access to secure sections. If an employee were to forget their ID card or forget to register for access to a different office, security number of verification methods they have to go through to identify the employee. In hindsight, none of these factors were something I truly noticed until I dove deeper into my cybersecurity courses. My initial training from the previous position was a three-week training course on how to navigate the multiple systems used by the company, understanding how to utilize the company’s private network to access resources and research materials, how to interact with clients, basic HIPAA laws and company regulations on how to maintain them. The training course was efficient in learning how to use the necessary systems, understand company policies, and set a solid foundation for my current position. Mock scenarios and consistent demonstrations were utilized to give new hires a more hands-on approach in learning how to use the necessary systems. Based on my understanding and experience, test environments of each system the company employs were developed to assist with wide-scale training while minimizing any potential risks of unauthorized access or affecting the integrity of clients’ HIPAA info. We were also given an overview of the company’s HIPAA guidelines to help us understand what was expected of the company and employees that manage said info. However, the training for my current position and skill development happened over a longer period. When I transitioned over, there was not as much of a training period compared to my initial entrance into the company. A part of that has to do with the position being an internal hire. The training period mainly made sure I understood the internal procedures and workflow for my team, but the technical knowledge came from parts of the initial training course, self-learning and exploration, on the job training for newer system in the previous position, and the rest came from parts of the cybersecurity curriculum at ODU.

Entering in as a new-hire, I didn’t have many expectations about the experience because simply I didn’t know what to expect as it was my first corporate job. However, when I entered my new position, I was able to gain some perspective about the sheer size of how big we as an organization are compared to the number of clients we support and serve. While I believe in the purpose of the company and understand there’s no malice in its intent, to be honest, I didn’t have the greatest impression about the organization due to some of the operational and business decisions I have seen made and how it has impacted both employees and clients alike, as well as how those choices were communicated. That being said, I do believe in certain teams and individuals whom I have met and worked with, that do support the company whole-heartedly which has improved my impression of the business to a certain degree and helped me understand that while an employee or member of any organization may not always comprehend the decisions made in a corporate bureaucracy, there is some substantial reason as why certain choices were made, even if they are always not agreed upon on a wider scale. Although, I do believe that my opinions are influenced by my time here as an employee and if I were a temporary intern instead, my perspective would be much more narrowed.

 The work environment and process-flow vary greatly in my current position compared to when I first started working. Coming into the company, I worked for a larger department assisting clients. Because of the sheer work volume my department had, our team had two co-managers that oversaw the team’s productivity, goals, manage expectations with other departments, etc. and two operations experts that assisted in the daily workflow and overseeing the individual members. There was a bit of micro-managing involved but it was understandable as the team needed to make sure that all inquiries were received and completed accurately within a timely manner. As an account coordinator, I currently work for a smaller team that supports the sales department that specializes in a specific health insurance market. In terms of hierarchy, it starts with our Director of Sales who below her is our Sales Manager that monitors and assists the sales team and my Director (of Sales Support), who monitors my team. Despite the standard hierarchy, both my director and her director have created a fairly, conducive work environment that is inclusive to all employees within our team and department. As a whole, our sales department hosts a monthly culture meeting facilitated by a volunteer from within the department that revolves around positive work culture and company morale emphasizing how we as employees can better serve our clients, coworkers, and company. Within a more focused setting, my director hosts weekly team meetings and bi-weekly employee check-ins with the explicit goal of addressing any work-related concerns from a functionality and company perspective in addition to confirming the state of our well-being and focusing on any personal concerns we as employees may have in and outside of work respectively. Beyond simply checking in, employees are also encouraged to map out their career goals and discuss their plans and expectations with their leaders. My directors have made it overtly clear their intentions to assist facilitating our career growth, whether that means our future lies with the same department or elsewhere. Assistance through encouragement, exposure, networking, and so-on have all been potential solutions proposed by management to better assist us in your careers. Being exposed to a work environment that not only nurtures our growth but promotes positivity and mental health within our personal and work lives enhances not only my experience as an employee but as a working professional and a human being. The uncontrived freedom we have in how we communicate between employees and management progresses the workflow which enhances our quality of work and thereby enhances the experience our clients have. However, I have realized simply being exposed to a healthy-work environment, alone, does not guarantee a productive experience. As an employee part of our job is to assist in maintaining that atmosphere for our coworkers but doing so means we have to acknowledge our actions and be mindful in contributing and utilizing work culture properly.

 The responsibilities of being an Account Coordinator on my team are constantly growing the more I work. Not all my responsibilities and tasks are IT or cybersecurity related but are pertinent in helping the department maintain functionality. One of the more technical responsibilities I have is assisting clients with generating and maintaining their user accounts on our client portal. A part of this can be verifying passwords follow the necessary criteria, authenticating users if they need to gain access to multiple client profiles, resetting passwords, and basic IT assistance if users have issues accessing the client portal. Some projects I have been involved in relating to these types of tasks would include hosting user demonstrations for your clients on how to navigate the portal and mass porting client accounts into new systems and profiles. The client portal is referred below in Figure 1. Aside from that, I also vet HIPAA and employer demographic information for new clients that are signing up for the specific medical market I support. Once all the information is verified, I upload and forward the data to one of the company’s subsidiaries that is responsible for the data processing involved in entering our new clients into the systems. A necessary part of that process involves tracking the progress of the data and verifying it is loaded into all our systems correctly. If not, then facilitating communications between the data processors and our department’s Business Developer also becomes a necessary task. One of the vendors we utilize in transferring client information to other systems and departments is known as Salesforce, refer to Figure 2. Aside from that, standard responsibilities involve making sure all HIPAA data is utilized, managed, and stored securely and verifying VPNs are updated.

 

Figure -2: External Vendor\_https://www.salesforce.com/

Figure : Client Portal\_ <https://employer.anthem.com/eea/public/login>

As it was previously stated, the skillset and knowledge that I currently utilize in my position is a culmination of experience derived not only from training and on-hands experience but through the courses offered by the degree thus far. Prior to beginning my job at the company, I had basic IT and office skills: I understood how to install software and updates as needed, typing, Microsoft proficiency, understanding of password safety rules, etc. Working for the company as I do, did not necessarily help me develop any cybersecurity skills compared to the courses in my degree, but rather it gave me an understanding of the concepts and topics that were discussed during my courses. Instead, the skill sets I developed pertained more to how to be a competent employee. A part of it was learning how to develop my own workflow without over-extending myself and working within the confines of a corporate environment. I have learned how to network with peers, potential business associates, coworkers, leader, and so on. Rather than learn about the importance of HIPAA, I have learned how companies such as mine manage and utilize client data which is something harder to teach in a classroom setting because it is such a private matter. One of the overlapping duties I have as part of my job function that coincides with a proper skillset is process improvement. This is something that has been regarded in ODU’s curriculum but not focused on. Understandably, it is hard to develop skills for process improvement until students obtain proper exposure which can only happen through experience. To my understanding, this is a topic that generally occurs later outside of a degree but is invaluable to keep in mind once exposed to as it was not a skill I had prior to my degree in ODU nor entering the company.

Admittedly, like any educational institution, I had reservations about how much I would learn during my courses that would become applicable to my career. If I were coming into the company as an intern, I believe it would have been easier to make certain connections between what I have learned in my courses compared to what is in front of me at work. However, because I started as an employee earlier on, I had to shift my mindset and focus more intently on certain connections at the start of this capstone course. One of the most direct topics that I drew knowledge from were the HIPAA laws and regulations that were consistently reviewed in the course. During my time studying legislations in the courses, the general focus was on making sure students understood the importance of these laws and what organizations were expected to do by utilizing this information. However, aside from knowing that, there wasn’t much else we could do in a classroom environment to utilize that specific information. Working for an insurance company from the technology side that services clients and supports the sales department, allowed me to see first-hand what tools and procedures are implemented to assist employees in maintaining HIPAA regulations. For instance, a browser tool is utilized by the customer service department to 1. Assist representatives in HIPAA authenticating whether the customer is allowed access to requested medical/ personal data, 2. If so, confirm what portions of information the customer is allowed access to, and 3. If not, what necessary information would be required from the patient to allow the caller access to the data. Beyond just HIPAA regulations, cybersecurity awareness and training were greatly emphasized in my lectures which I saw first-hand how companies attempted to implement said training. The importance of it versus how generic employees view it leave much to be desired but reinforced why it was so important to understand in my courses. And finally, the one of the most important lessons I took note of as it was being taught during the program was seeing how businesses set-up digital and physical security: the use of VPN’s to secure access to networks, the repetition of updating employee passwords every few months, utilizing numerous passwords for varying systems, BIOS updates, access control policies put into action to reduce unauthorized access, restricted physical security access to certain regions of the office, strategic placements of hazard prevention to reduce vulnerabilities (generators, ventilation, security cameras, flood lights, multi-point entry), etc. All these concepts while simplistic in nature were consistently taught, enforced, and reinforced regardless of the course because of its importance, but it wasn’t something I initially noticed about my company or office, until I had the opportunity truly focus and make those connections. In that manner, ODU’s cybersecurity program has greatly prepared me for understanding all the necessary precautions a major corporation may take to reduce risks. It is not something that is generally noticed at first because I believe in general, you expect a large business such as Anthem to implement proper security procedures and precautions. Yet, the one thing that is not spoken of during courses which may be useful in the curriculum is advising students how to approach leadership in improving security from an application standpoint. Some of my courses have allowed me to do mock scenarios in exercising this action but I believe it is a bit different compared to a real-life work environment.

Admittedly, while working at Anthem is a worthwhile experience and being able to experience it while keeping the mindset of an intern in consideration relating to ODU’s curriculum, not all the learning objectives were met. But even so, by not meeting certain objectives, I was able to gain a perspective that may help me in my next endeavor. To start, the most basic objective I had was to gain a better understanding of the industry. While I do not work for a tech company, I did develop a better understanding for the health insurance field and what place technology and cybersecurity have in it. My time at the company has also allowed me to the witness the short-comings of how data is processed in modern times and the need to better address those short-comings using technology. My next objective was to gain a better understanding of the legal cybersecurity requirements that Anthem is required to uphold. In that regard, I have had the privilege of being exposed to how the organization adheres to there laws. I have utilized the internal HIPAA tool that is made available to the customer service department which has helped me understand the more detailed aspects of HIPAA. For instance, in our courses, we have been taught that HIPAA laws are made to protect the health and identification data of patients. Within those parameters of protection, we learned how an organization is expected to manage and protect that data. It goes without saying that the patient, provider, and health insurance companies would be privy to that information. However, working for Anthem has also taught me there are various third parties (such as brokers, insurance agents, etc.) that are privy to that information as well, within proper authentication and reason, and HIPAA has guidelines on how outside parties are able to obtain that data. My next objective was to build a better understanding of technology and cybersecurity needs in non-standard settings (for example the sales team). This objective I feel has only been partially completed. Through my responsibilities in supporting the sales team and clients, I have noticed the lack of basic, technological understanding certain people have. While it is harder to assist clients in this regard, though not impossible, training and assisting employees in overcoming these shortcomings could prove useful in not only productivity but security as well. In other regards, it’s a lack of proper utilization of technology due to the difficulty older companies have in transitioning from one system to the next. The availability of resources and ability of the IT department to implement these changes are a separate matter, but I believe that as technology continues to grow, it is the responsibility of organizations to adapt for the sake of their clients. I say this goal is only partially completed because I did not get as much exposure to other departments as I would have liked since I mainly support the sales teams. My last objective was to get more exposure to cybersecurity aspects in corporate settings. While I did get to see traditional cybersecurity counter measures in application, as previously explained, I wished I had a more focused opportunity in seeing the more complex nature of the field. Regrettably, that has more to do with my job function that the experience itself. However, I was able to see how HIPAA and cybersecurity violations are reported and directed within the company in addition to speaking with certain security technicians and advisors, which does to some degree give me the exposure I was hoping for.

 While this is a job and not an internship, there are interesting and exciting characteristics about my experience as well as negative ones. A part of it is how fortunate I have been to have such encouraging and supportive leaders to have allowed me the exposure I wanted for my education. Of course, for security factors, I wasn’t going to be exposed to everything that I wanted to know but the freedom I have been given thus far is amazingly valuable. As well, the validation of being able to make certain connections to what has been taught through the curriculum versus what I have witness implemented in a corporate setting means there is purpose to what is being taught. The most discouraging aspect of my experience is most likely working with clients. Not all interns or jobs will require someone to work for clients, but it comes down to the nature of the job and what role a person is hired for. Dealing with clients won’t necessarily always be a negative experience but it is something outside of our control which isn’t always the easiest fact to accept even though it is necessary. The most challenging aspect I would say has to do more with being able to contribute the way you want to. As an intern, and even as an employee, we’re always encouraged to contribute what we can for the betterment of the team and the company. However, it also must be done within reason and proven to be useful to coworkers, leaders, directors, etc. I feel some of us as students may always be too eager to prove ourselves and wanting more responsibility. But understanding that form of trust comes from experience and time. Being patient in knowing when to do more and when to do what your told can be hard to accept at times. And even though I came into the company as an employee, I feel that is a good mindset to have going into any internship, managing expectations. Whether those expectations are focused on the job function, the experience you want, or yourself as an employee/ intern, it’s helpful to be realistic and understand what is within proper founds of action and what is not. If a student has trouble in this regard, the biggest advice I can give before starting any job, internship, or degree is be willing to communicate. Facilitating communication, asking questions, and giving opinions can be useful in learning to manage expectations and get the most out of any experience.

 It was more interesting to experience my daily life of work with the mindset of an intern. Having the ability to see your work environment from the perspective of a student allowed me to meet some of my learning objectives while also validating my time as a student was not wasted in going through the curriculum at ODU. I came in through the company without much knowledge or experience in my opinion but being able to utilize what I have learned in my classes and helped in building my confidence and experience in the workplace. I have limited time left as an undergrad student but my continued work at Anthem may prove useful should I choose to pursue a graduate degree or even acquiring certifications later. In terms of future career prospects, having a corporate experience and gaining an understanding of where my knowledge and time will be utilized will help navigate the potential career paths I may take for better or worse. But, without a doubt, my time as an employee, and as a student, was not and will not be wasted.