Interview with the Information Security Department

Rusty P., Alexi M., Obiora O., Xavier G.

Director, Manager, and Analysts for Information Security

June 1~18, 2026

Interviewed by: George “Trey” Smith III

CYSE 368

Summer 2026

Professor Teresa Duvall

TA Jade Hines

While this assignment is usually meant for one person to be based on, I had interviews with my entire department to get a better understanding of my coworkers, and also build a better relationship with them. With this being said, there is a ton of overlap among all of my coworkers. I also added my own question to the interview for more clarity or to satiate my curiosity.

I want to expand on why I interviewed my entire department. Since there are only three people, plus my director working in the information security department, it was fairly easy to interview them. I was severely interested in their answers to the questions. There are a lot of different people from very different backgrounds in my team, despite being so small. My director has been in the IT/Security industry for over 3 decades. My mentor was an intern at Chartway just like me.

During the interview process, I started with the question: how did my coworkers get into the Cyber/IT field, and how has this field encouraged them to get more

certifications? There were a lot of answers I got from this question, but most of them coincided with the fact that someone helped them think or learn about an IT role. My coworker Obi (a junior information security analyst) highlighted how one of his high school's advisors asked him a blunt question about what type of games he likes to play. The choices included activities such as Minecraft or chess. Obi stated he loved to play chess. His advisor led off by saying cybersecurity would be a good role for him based on that answer. From what I gathered, the underlying theory of the ever-evolving game of cybersecurity is adjacent to the game of chess. My director, Rusty, was mentored into the field at the Naval Academy and expanded from there. These stories really resonated with me because I wasn't too familiar with the concept of cybersecurity as a field. Growing up in Newport News, all I ever heard of was Computer Science. I had actually had a crazy encounter with someone learning ethical hacking that essentially changed my life forever.

My additional question on the encouragement for certification was also insightful. My mentor, Xavier, highlighted that being at Chartway, which is his first fully cybersecurity job, has helped push him to get more certifications, such as the SC-200 and AZ-900. He said that the shift into a security-focused environment had shifted his focus to learning more about the tools and environments he will be learning, to stay relevant in the field. My manager, Lex, highlighted the importance of staying relevant in the field of cybersecurity more. Since the field of cybersecurity is ever-changing, he talked about how certifications are one of the most provable forms that show you are trying to keep up.

Next, the question asked was, what would be the most important knowledge, skill, and ability needed by someone in this field? Tagging onto that, if you had gone back in time and had to do it again, what would you use? Out of all of the interviews I did, the skills that were recommended were IT and Networking basics, Critical thinking, and the ability to pay attention to the smallest details. While the first one seems very basic, I have found that it can be the thing that makes or breaks you from being a step ahead within this field. When I first started my own homelab, I was extremely lost when setting up my own firewall. This stumped my personal learning and progress for longer than I would like to admit. Once I put my foot forward to actually learn the environment and protocols, the systems I was interacting with during my later activities came more naturally. Next, critical thinking is one of the pillars of cybersecurity. My director and my coworker spoke about how vital it was to have good critical thinking skills. This skill enables and contextualizes the final point of seeing and understanding the smallest details. While small details are usually something that is nice to notice, but acceptable to miss, cybersecurity is mainly focused on ensuring nothing is overlooked. Due to the interconnectedness of networks, even the slightest shifts of logs or script activation can show indications of compromised security. If we as cybersecurity professionals miss something like this, worse outcomes are more probable to happen within the network, which can affect the company.

After that, we have my question: if you had to go back and do it all over again, what would you do? This question had a lot of diverse answers! Obi responded by increasing his social network early to ensure his achievements and efforts would have a greater outreach. My manager said he would have gone to more social events, but also

read over more vendor documentation early to gain a better understanding of tools and environments. Lastly, my director stated that they would stay on the same track of mentoring and expanding their outreach after the academy. I really like these responses because they showed me that while the times when my department was starting were different, the methods of learning and interacting are essentially the same. Learning still requires talking to peers and reading professional documentation, which are vital to gaining a higher level of understanding in cybersecurity. Expanding your social network and conversing with others is also needed to stay a step ahead of others within this job market.

Now, the next question is: what are some important soft skills you have found to be the most important and why? This is the question that generated the most similar responses. That response is effective communication. One thing I am told over and over again is that cybersecurity generates no money. Speaking purely from an internal company side of things, cybersecurity takes money to protect assets, which can be seen as a net negative to some companies. With this being said, an effective communicator on a cybersecurity team can shift perspectives and highlight the importance to the executive-level staff and board members. My Director and coworkers have stated that being able to uncomplicate and display information is vital to displaying work done within the company to high-level staff.

The last two questions I combined together, which were: What is a good entry-level position to get to your position, and what are you looking for in a full-time candidate. I am combining these two because the first question was a unanimous IT support/Help Desk role. The reasoning is that the ability to troubleshoot, implement, and

help resolve daily issues within all technological areas helps expand your knowledge to one of the highest degrees.

The next question, I split into two perspectives. First, for my co-workers, Obi and my mentor, Xavier: What qualities are you looking for in a co-worker, and what was stated above for Rusty, my director, and Lex, my manager? The responses resulted in someone who has a hustle to learn more about the field, someone who is open to communication and is willing to bounce ideas off of, and someone who works well with the team and can help out. As I reflect on my previous 150+ hours of work, I believe I do fit the criteria of the first and last suggestions, but I still feel like I'm lacking with the second one. Coming out of my shell and cementing myself with the team is something I strive to work harder on within the next 5 weeks.

I just wanted to take the time to also shout out my amazing department for helping me out with assignments. I really appreciate them and all their help in sharing their experiences with me. Obviously, I couldn't do it without them, but outside of this assignment, they have helped me and encouraged me throughout this entire process. This has severely helped with my anxiety about working in a corporate environment.