2:15 PM

Interviewer: it is nice to meet you. As I said on the phone this should not take more than 20 or 30 minutes. I really appreciate you taking the time today to meet with me and allow me to interview you on cybersecurity. I was hoping that we would get along great because I also have a cybersecurity degree although I admit I ended up teaching and finally running MIS but we have similar backgrounds.

2:16 PM

Respondent: no problem, I knew you had a cybersecurity degree because I heard other people talking about it. Do you have any certifications?

Interviewer: no, my interests were always academic, and I just never had enough time to pick up some certifications together with the degree. Speaking of certifications which ones do you have?

2:16

Respondent: I have the certified ethical hacker and the comp Tia Security+ certification. What I really want though is the CISSP. That is the certified information systems security professional. If I can get that one. If I can just make the time to get that one I can get a job anywhere making well over six figures.

Interviewer: Those would be really nice to have. My first question is why do you choose the occupation of cybersecurity professional?

2:22 PM

Respondent: Eh,well, I grew up in the 90s and really enjoyed watching movies about hackers. Think it was about 1996 or so the movie antitrust came out. I do not know if you saw that one or not but it was about a hacker who was recruited to company and he ends up finding out that the company is extremely corrupt even involved in murder to advance its technological goals. The main character a guy by the name of Milo also finds out that even his girlfriend from college was planted by the corporate company to entice him to work for them. There was a really good movie. Anyways, I started thinking about programming as a career. I know it seems kind of weird getting the programming because of the movie about coding. These days almost everyone I work with got into programming because they wanted to write code for computer games I feel like the computer world is been saturated with gamers or wannabe gamers. It is kind of funny if you think about it because there really are not that many jobs for gamers and so these kids are out of school pick up a couple languages and can be gamers cannot get a job and then end up working for some IT department.

Interviewer: that was really fascinating so did you have other influences that pushed you into the field of cybersecurity such as family members?

2:25

Respondent: my parents did not understand what cybersecurity was and remember it was not really a term back then. The only thing they understood was that I wanted to get into computers. Of course, in the 90s computers had just gone mainstream with Microsoft putting out the Intel chip and homes getting Internet connections. You might remember the old ISPs that used your phone connection and get a baud rate of 14.4 or something. If you had told me back then that I would be sitting at home playing video games on an Internet connection of over a gig I would have said you were crazy. I still cannot believe the advances in technology that we have in our homes today (silence).

Interviewer: can you tell me a little bit more about the role your family played those specifically her parents?

2:29

Respondent: oh yeah, sorry I have a lot on my mind I was getting to that. I do not really remember my dad saying too much about it he was a tabular going to college since he had not gone. My mom on the other hand she was really excited about me getting the computers and kept telling me I was making a great decision in the mid-1990s computers were still exotic to most people. So yes are going to college and be encouraged to study computer science was definitely encouraged by mostly my mom. But remember nobody was using the word cybersecurity back then,

Interviewer: that was really interesting could you please walk me through a cybersecurity incident that you have had recently?

(Takes time to answer, thinking)

2:30

Respondent: well, I am happy to say that we have not had any major cybersecurity incidents in the last few years. That is not to say we are constantly harden our systems to defend against an attack. So the incidents that do happen are isolated to a small group of people or usually just one person. Couple months ago we had a student claim that there are student account had been hijacked. I checked all the usual security applications looking for a breach by I did not see any alerts or any red flags. Did notice that the IP address that had looked at her account did not match the IP addresses that she had been using. It turned out that another student had guessed her password and accessed her online account. This kind of thing happens from time to time and it is almost always the end-users fault because they do not follow good password protection protocols. We only recently started to offer two factor authentication which adds that extra step four accessing accounts. But it is difficult to please everyone because now there is just one more thing that an end-user has to do and they forget their security questions/answers. Thankfully though we have not had any major breaches especially toward databases or networks. That is mostly due to the fact that we keep those locked down really tightly.

Interviewer: how did you react to the incident?

2: 35

Respondent: whenever this security calls coming in I do feel my heart rate increase laughing. My biggest fear of course is a full breach of our databases. Especially with the ransomware attacks that happen all the time these days. And even though we do everything we can to prepare ourselves for this type of breach it is never enough, and they could still happen. So the usual step is to check the software and look for an indications of a breach. After that, I look at the IP addresses see if anything unusual happened. Later, I need to talk to the student or the person who reported the incident. Try and find out everything I can about what happened why they think it happened you know the usual stuff. In her case she been locked out of her account so she could not change anything on her own. But once I validated that she was who she says she was then I opened up her account and changed her credentials and helped her set up two factor authentication. I also explained to her the necessity for a more complex password. In her case she volunteered that she had used the same password for her other accounts so that we would be easy to remember. Of course you know that the major major no-no. She was really lucky that the person that had locked her out of her account had not thought to try to access her social media accounts or she would have had a real nightmare on her hands.

Interviewer: How did you work with administrators to address the incident?

(Silence, thinking)

2:38

Respondent: