Annotated P1 Interview Notes

## **Job Role (Data and Security Manager)**

* How do you feel about your job?

I am an assistant network operator and security manager. I hold an applied Sciences degree, robotics specialty, automotive industry, but I never worked on a robot. My day jumps from this to that for 21 years, Everything that is wrong with the infra.

* How is your team organized and how does your team cooperate with other teams?

The team is me, myself, and I. I would love to get someone to do the grunt work. When they have problems, they directly come to me. I almost work 24/7 because I can’t allow the server or the database to go down, but it can happen at any time. Today I am busy, tomorrow I am not.

* So you help out other individuals? What kinds of help do you provide?

Yes, I am a salaried employee. If one of the servers goes down, I am usually one of the people that comes to fix them. My employees know that they could call me until 10 PM. Starting at 6 AM, and weekends.

## **Transition**

* Why and when ADMI started the transition?

About 5 years ago, we started moving onto the cloud. What prompted this is the natural convenience of ADMI. The intrusions of the rest of the world. People like “strip kitties, they would come into our DNS. I let solutions like GoDaddy take control over it. I don’t have to worry about the bandwidth.

* Can you provide more details about what you’ve done in the transition for now?

We started seeing that our home domain, and the front of it, not any other domains, they started to try and hack it. That one is now on the cloud. We made it simple, we don’t have people trying to hack the page.

* What’s the difference between the local and cloud management of the security issue?

Offsite servers are treated as my internal ones, while for the cloud servers, I don’t have to worry about intrusions to that particular code. The log files are looked after by someone else. Not too much teaching to my employees. Cloud management do save me more time and efforts

* How do you like the transition so far? Tell us about your concern.

It’s a long process. I am the person who has to make the physical infrastructure happen. I am the one deciding how that works. The rest of the developers interact with it being on the cloud. There are certain things we could do, others. One of our servers is Oracle, and it is protected with Firewall.

Data import from the employee house took so long. He had to take the data and transfer it onto the internal domain.

The second thing is that if we have a fresh server, we run into issues. We have troubles with licensing, especially when you’re using them on VM environments.

The third thing is we run cold-fusions. That is not too much of an issue. Not housed in our internal domain. Taking the code and taking it off-site with the front-end and back-end. The code would probably break because I don’t know how it works remotely. It would be connected to an off-site. We have to figure out what is going to break.

I foresaw a lot of problems like the coding break.

## **Security**

* Could you please walk me through the security protocols now? Are there any guidelines or documentation?

There are different protocols in different scenarios, you need to specify one. Physical, software, or network?

* Let’s start with the physical one then.

I get audited, there are specialty teams. We will talk about keys. There are 3 current keys and a motion detector in every room. We have security on all the doors. If someone breaks into the building- security protocols are instant. There is an alarm system and 2 individuals from ADMI & police will come. There would be a second step if they got into the server room. We will physically unplug the server.

* What about software?

Between each of the servers, there are only certain ports available, so it can help with prevention. There is a switch level to turn all of them off. Beyond that, there is a firewall set up with Comcast. It’s basic, so it is our firewall that I have set up to prevent traffic from all countries where we don't have business around the world. This firewall prevents 80% of traffic from coming in. I see no reason to have this traffic.

* What’s your emergency protocol?

Call P1 and see what is going on. Most people don’t know how to fix it, so I need to make a diagnosis. For example, when the Oracle database is not working, they’ll contact me, and I’ll try to log in remotely. If it can’t work well, I’ll come to the server room.

* How do you store your code and data?

We use an oracle to store data and Github to store code.

* What about the database?

If someone gets into the database, it’s worthless because the database is encrypted. Oracle If the database is not responding. I will remotely log onto it. Is the network still up? Do you see a light on the modem? I’ll provide remote maintenance on the phone.

* What about cloud security for now?

Off site-we have DNS. I don’t think we will have problems with GoDaddy. Then we have AtlanticNet. That server is imaged on a daily basis. If that one went down, they would restore the image. Those would be our off-site.

## **Data**

* Would you please talk about some details about the data flow, I’d like to know how it works.

I am a part of the data team. I could make computers communicate with each other very well. I move a lot of traffic. I moved Ford's data from their database to ours.

* How does the data flow between your company and the customers?

We only upload data manually, and there is no interface for other people to upload data. There is code there to prevent bad code from coming in. Data is encrypted on the fly. We foresee a problem with having the front-end and back-end of the environment.

* What part of the data has been transferred to the cloud already?

The main part is the DNS and our website.

## **Difficulty and Observation**

Sorry, I am at a meeting and I am requested to fix equipment in the conference, and I may leave for a moment at any moment.

* That’s totally fine, this is what we want to observe! So what will you do?

I have one individual, and I remoted into his system. If he doesn’t log into it within 5 minutes, I'll try to fix the issue. For me, this may just take minutes, but for him, this is an emergency, because it means he can’t work all day. Prior to our meeting, I was in our IT meeting, we have a discussion about what we could

* In your experience, how did you deal with a data breach?

There was no data breach before.

* But what if there is one happening in the future? Or what if another data issue happens?

There is another one that happened 15 years ago. I'll physically disconnect the server from the network, and see what the breach was. Then I’ll restore the system to an earlier version of VM, and update the code. Afterward, I’ll apply the fix and test it. Finally, I’ll publish it to the public.

* What if an issue happens again and again? What will you do to solve it?

There is no issue that happens again and again. Every problem is different, and I solve it when I meet one.

## **Colocation**

* Would you please help me develop a mental model of how you perform colocation?

We don’t do colocation right now. We have 3 things on the cloud, website, VM on AtlanticNet. Finally, we have a spun-up Vm that houses. It runs a version that is called Fusion. I would have it back up in a day. 24-72 hours of the DNS. (Propagation of DNS)

* How will colocation help you?

Other people would be responsible for fixing hard drives and such. I wouldn’t be tasked away with.

* What partners do you want to work with to co-locate your servers?

There are mainly two ways for colocation. You could lease their equipment or let them take care of your equipment. I prefer the latter option because we would only have to be responsible for the software then.

* How many companies provide those services? How would you choose among them?

Only Dells. Because all my servers are Dell now.

* How will you ensure data security when your servers are co-located?

I can’t set up security protocols until it’s in place.

* What if an accident happens with your partners? How will you deal with them?

I can be a bandaid. I know about the infrastructure and how it works. When people have those types of issues. I could be a part of helping fix them. We only have a couple of people who can help fix the Oracle DBA. I don’t have one major issue that happens all the time. If I had only one issue, it would be fixed.

## **Lift-shifting**

* Why do you want to perform lifting and shifting now?

I hope I don’t have to maintain configurations of the workflows.

* What’s a specific problem that you want to lift or shift?

Our team is growing and included in the coding process. I don’t see any issues in our infrastructure of people.

* From the standpoint of the manager of the whole company, what is the current stage of the cloud transition process in your company?

Upper management does not have a full grasp on what it would take to move onto the cloud. That is one of the reasons to participate in this study. Give us a pathway to move to the cloud. I don’t have that pathway, because there is not a pathway. The pathway is there, but when presented with all of the items, they are not understanding what it would take. As much as they want to understand.

**Reflection**

This is our first interview, and we’re a bit nervous about it. Fortunately, I think we did make constructive communication and gather a lot of information that we want. Through the interview, we learn three main challenges faced by the ADMI IT department as well as the issue in management. However, there are still many aspects where we can make further improvements, ranging from our preparation to spot performance.

Firstly, we should do some background research about the interviewee’s job in the company before we started the interview in case that we don’t understand the answer. It happens a lot of times where we need the interview to explain the term he’s talking about or we just skip the details about the term he’s using, like cold-fusion. It may waste a lot of time and prevent us from understanding the answer quickly. On the other hand, we don’t know the scale of the company, as the number of managers or the number of members in a team. This information is very basic and important for us to get a general picture of the company. However, we missed it, and even forgot to ask it during the interview.

Secondly, when the interviewee gave us a surprising answer, we’re a bit at a loss and don’t know how to proceed. For example, when the interviewee said the team is only himself or there was no data breach before, we went on other questions instead of improvising questions to get further details. In my opinion, these answers are very important because there must be more detailed reasons that make it so counterintuitive. We should expect that answer before the interview and make a more comprehensive preparation for it in the interview protocol so that we can deal with the interviewee’s answer better.

Thirdly, we didn’t control the interview time well so that we can’t make further questions based on the interviewee’s last answer. When the interviewee pointed out the problem with the manager level, we didn’t follow up due to the time issue. However, it’s an important topic that is worth discussing.

To sum up, a lot of problems are caused due to lack of experience. To make further improvements, we should make a more comprehensive preparation, and try to be agile during the interview. The interview also needs to have stronger control of the interview.