Q: [GQ1] In which sector does your organization belong to? What are the activities of the company?

R: It’s the IT sector. We are a SaaS provider, we write software that people access via their web browsers, it’s for big corporations. [DESCRIPTION OF THE SERVICE PROVIDED BY THE COMPANY]

Q: [GQ2] What is the number of employees working for the company?

R: [BETWEEN 10 AND 100]

Q: How many years has the company been operating?

R: [AROUND 10 YEARS]

Q: [GQ3] What is your current position in the company?

Head of the IT department

Q: [GQ4] Is there someone (or a certain department) in charge of security management?

That would be this department. We’re in charge of the technical security. In an organization, everyone should be responsible for the security, the people taking care of their laptops and they make sure they focus on their personal data. That’s not a technical problem, that’s procedural teaching education.

Q: Yes, but there would be a department in charge of putting those internal rules.

Not for a small company typically.

Q: But you try to make everyone conscious

R: I’m one of the people that would help to educate, yes.

In a company like this, there are 3 people that deal with contracts and the office management, so insurance would only come through that department. Typically, it would be more to do with consents, protecting the building from fire for instance. The common and mandatory ones. I guess is possible if one of our customers says, “we are interested in buying your system, but we want some protection if you were to leak our data”, maybe the pressure would come from our customers and the contracts department would say “we need to get this in place in order to show it to our customer”. That’s the typical way (if we were to get started), that would be my guess of how a company like this would be interested.

Q: There are liability insurances for these cases, if a company comes and says, “I want to be protected for what I’m getting with you”, does that exist?

R: It’s a contract by contract case. When we engage with a customer, sometimes there are additional things requested, sometimes not. There is a negotiation of how much liability would be passed down.

[Since scenario IV does not apply, the interviewer tried to make enough questions to “cover” both scenario III and IV]

Q: Does the company takes care of itself regarding IT or do you have IT services outsourced?

R: We generally take care of ourselves, but we do have some partners consultants, all our software is deployed in a public cloud operation [NAME OF CLOUD SERVICE]. We have consultancy and monitoring services from our partner. We are responsible for it but sometimes we refer to their expertise.

Q: [Q3] How did you first hear about cyber insurance?

R: I’m aware from the reading press, I know it exists but it’s not in the front of my mind.

Q: What’s your idea of what is cyber insurance?

R: Is like any type of insurance where you pay a premium on a longer basis. If something bad happens is going to cost the company money and it can make a claim on it. I guess there would be a loss of reputation if there was a data leak. Our policy says that as soon as we are aware that we have to let know our customers straight away, then it becomes public domain. That would mean the loss of reputation, that could be several weeks of stopping what we´re doing from a technical point of view, to clean up the mess and change what we’re doing. If a bad thing happens I expect there would be lots of costs incurred. Some of the contracts with customers might have a claim, a clawback. So, I’ll be guessing the cyber insurance policy would help cover those costs.

Q: Do you know companies who already have suffered a cyber attack?

R: No personally, I’ve only read a lot of stories in the press.

Q: [Q6] What factors make or could make the company more susceptible to security attacks?

R: There are two dimensions, the technical protection and the other one more procedural. I think a lot of people think of attacks being done by bad hackers and my impression is that most data leaks are caused by people being careless with passwords or putting sensitive data on a laptop, that’s an easier way of getting data than cracking an Amazon cloud system, for example.

Q: What do you think would motivate these people to get information from a company like this? What reasons would they have?

R: The bad buys are hopping for financial information, like passwords to get access to bank accounts. I guess is possible there are more targets in the industrialized sector, targets on companies to get their secrets. But from my experience, that’s not how I see. If a company like this was to get attacked it would be part of a general phishing from someone trying to get useful information, hoping to crack a database and see what’s in there to make money from.

Q: You don’t see that the activities in the company are of high interest for others to bother on attacking you. Do you deal with personal information from your clients that you have to take care of?

R: We do, is not the highest grade of personal information. There is no credit card details or medical history. The most sensitive information is [DESCRIPTION OF DATA]. The risk is that we would pass on contact details. I don’t think that anyone understanding the company’s activities would target it as a high-value target. But, people phish, and they just hope they get lucky.

Q: [Q8] What are the main security threats you consider relevant to the company?

R: The most common is the data leak. And, if your customers don’t trust you that you can keep their data secure, then you’ll not be in business for very long. There are other types of attack but, things like bitcoin mining where they want to get on your servers and use your CPU power, it’s embarrassing if someone could do that but it’s not going to make a reputational damage like a data leak.

Q: Do your customers ask for some kind of liability with the information they have with you?

R: I don’t know much about this because I’m not in the contracts department. My understanding is that most customers will ask for some coverage or guarantee. A small company like this could not be in a position of covering millions of dollars in damage.

Q: [Q10] If cyber insurance was to be offered, for what reason you would not get the cyber insurance?

R: This is a personal opinion. Having had the experience with insurances like car insurance or house insurance, knowing how difficult is to claim based on small things like “sorry, your lock wasn’t the right”. I’ve seen lots of claims bouncing and being lost due to small reasons like this. So, I couldn’t begin to imagine how this would look in a complex situation with a cyber insurance claim. I have low confidence that a claim would be successful. With a house you won’t get a compensation because you left your door open, then how could you have that conversation about a complex computing system? I don’t know how we could satisfy an insurance company with the due diligence for keeping things secure.

Q: [Q4] Do you know companies that have a cyber insurance?

R: No

Q: Let’s say that if you were to adopt cyber insurance but other companies don’t, especially companies you have contact with, would that be a reason for you to not get cyber insurance since your covered, but they are not, and the damage could come from them?

R: No

Q: Price could be a reason?

R: Price is always relevant. It would be down to whether is good value. There would be some value by showing our customers that we have this kind of coverage and to know if that would make them easy to sign a contract. That’s worth something for the price we’re paying.

Q: Do you have a role in the company related to GDPR?

R: Yes.

Q: Cyber insurance could be seen as covering part of the responsibilities you have with GDPR.

R: We spent several months leading up to May, preparing for GDPR. We’ve been talking about data security, GDPR is just part of that data security. Is not a brand new thing, it was just an extension of the data security principles we already have to have in place. It’s relevant, but it didn’t change the game for us. The big change with GDPR is giving visibility, it brings notifications, letting people know exactly what you are going to do with the data and give them the right to change their mind.

Q: [Q7] What protective measures do you have in place?

R: All our software is in [CLOUD SERVICE NAME] and we have strong policies for not taking the data out of [CLOUD SERVICE NAME]. It’s not a hybrid system, we don’t have our own data center. We never leave the cloud basically. Under special circumstances, if something is needed because we have to satisfy a customer by extracting the information, we immediately delete it, within a business day. Those are the main protections because [CLOUD SERVICE NAME] has a fantastic physical protection. If we were to have computers here, proving that we didn’t let any bad people in the building it would be a big challenge. The fact that it’s in [CLOUD SERVICE NAME], means that the physical security challenges disappear. We still have to make sure that our software is secured against hacker attacks.

Q: When you get the [CLOUD SERVICE NAME] services, did they show you how secure it is?

R: No, [CLOUD SERVICE NAME] is a [big] business. They don’t need to show it. They show pictures but that’s it.

Q: [Q11] Are there additional security controls needed to be implemented?

R: Every company could always do more. Then it comes to a balance where it’s cost effective. I’m not aware of any security breaches that have happened in the history of this company, so the measures that are in place seems to be in good balance. I could always think of theoretical attacks that could happen and pay the extra money and extra time to guard against them.

[Q12 is answered in the previous question]

Q: In the short term, are you planning something?

R: We have projects ongoing, which will continue to improve our security. Is not something that you do and then stops, it’s an evolving process. But there’s always an extra level you could go to. You have to take into account the kind of business you are, are you storing medical records? Then there are bigger things you could do to keep them safe.

[Q13 is inferred to be answered from the previous question]

Q: [Q14] What would motivate you to get a cyber insurance?

R: If we found that we have been compromised, that there has been a breach, that would make us think that our security needs to be stronger, we would obviously work on protecting it. But, in the meantime, we need to cover ourselves until we show that we have worked on this. That’s one scenario. The more likely scenario is customer pressure. If we’re about to land a big deal and the big customer says that they would only sign if they see that they are covered for a certain amount of compensation in case of a breach, and we’re not able to negotiate that, then we would act to get an insurance for this.

Q: Do you know how often is that insurance companies approach you to offer new products?

R: I’ve been here for [NUMBER] years, I have never been approached by an insurance company.

Q: [Q15] Do you know about the premiums price?

R: Not a clue

Q: You’ve seen in the news the type of cyber attacks that happen, do you think this is because they are looking for a specific sector, market or companies? Or is it randomly?

R: I guess is more likely if you’re a high-value target, but I’m not complaisant, I know there are a lot of robotic programs that are just scanning the Internet looking for machines, they ping the machines questions about what their type of software, depending on what they get there are some vulnerabilities n certain type of software, so they scan a million machines and 50 of them with a certain combination of software that is vulnerable, so they will try to get inside those machines. Once they’re in they look for information, maybe they hit the jackpot, maybe not. There are a lot of attacks like that. Is not random because they are hunting for vulnerabilities, looking for vulnerable systems but without knowing what’s in there.