Q: GQ1. In which sector does your organization belong?

R: Financial services

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

R: [BETWEEN 100 and 150]

Q: What is your current position in the company?

Head of internal services

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

R: Cyber security or security as a whole?

Q: IT security

R: Yeah, we have an IT manager but is one of his tasks. He's not dedicated to one task and he is the one I consulted

Q: Is he internal?

R: Yes, he is internal

Q: You have known a cyber insurance, for how long?

R: 4 months, recently. At the beginning of this year, I consulted it with the owners. I proposed to them that we should consider a cyber security insurance. They asked me to compare different offers, and I did, and I spoke to different persons about it, and I consulted my IT manager. Then we decided to arrange this.

Q: Q1. Do you work directly with the insurer or the broker?

R: The broker

Q: Have you already worked with them before?

R: No. We have several brokers because we have different insurances and we didn't work with [INSURANCE BROKER COMPANY] before. I compared them with another broker we use a lot for other liabilities because we also have a big insurance for professional liability but they had an offer that was not very competitive.

Q: At some point did you think that the professional liability would include the cyber insurance?

R: Yeah, I discussed that because that was one of the questions I had. Is this something that is extra or is not included in other liabilities? Because is a liability and insurances are for liabilities, but they excluded it. It was new for them and they were sort of old-fashioned and that's I we decided to do it in another way. This is new, is not included in other liability insurances, not yet, and that's why we choose it to do it in this way.

Q: Q3. Please describe the process for selecting and buying cyber insurance with your broker and insurer.

R: The broker approached me about cyber security and I asked myself, is it something we need? Because I'm in charge of internal affairs and policy insurances, I approached the guy who is normally in this office, and by the way, he was in the professional liability insurance, and we discussed it. He first said he's not aware or don't know anything about it, so I thought ok let's have some research and then I was approached by several parties and by [INSURANCE BROKER] because it is a topic that pops up. Then I investigated and talked to my IT manager to discuss what could happen. This was one year ago.

Q: When did [INSURANCE BROKER] approached you?

R: Yes, this took a while. I also discussed it with the IT manager because last summer we migrated all our data to the cloud, that was also a moment to contemplate our liabilities, is it not wise to have an assessment of the danger? Because our reputation is all we have, we can't afford to be blackmailed, we have to be very precise about this, and that's what we do in IT. We also have to get the best advice we can about what possible dangers we might encounter. So that's the reason why I was also instructed by the owners, what can we do? What are the possibilities? What are the dangers? What is wise to do? So we started with different brokers, we had this broker we normally use, we have [INSURANCE BROKER], and it took a while.

Q: So, it was a serious of talks coming and going?

R: Yeah, about what do they have and how can we compare different offers, different brokers? In the end, there are not many brokers that offer an insurance from one of the big companies, and there are not that many big companies that have an interesting offer for a company like ours. I think there are only 3 options. Then you choose, and the broker offers choices. One of the reasons why my broker convinced me was that it met our needs at a price that was ok at that moment because you never know what is going to happen. The price could go up because of new dangers or something like that, so we said ok let’s do it. Then I talked to the owners and we decided to go ahead, and the IT manager was also involved in the process. The next step is to have a backup plan because an insurance is nice but that’s only if anything goes wrong, and you have to also prevent that something goes wrong. One of the things that happen with insurances like for fire damages is that they have demands to implement, else they won’t give you an insurance. So, that’s also one of the reasons to have an insurance is to be aware, be alert, to some of the dangers and the implementation of this new law, GDPR, because of this new law we have new regulations in our company and that’s also good for cyber security reasons because you have to be aware, be alert, on what you do, what you don’t. Another risk is that you have contact with your clients and possible dangers from your clients that will be incorporated in your systems, that’s the way to have new relations with your clients and suppliers that is affecting your cyber security. After this, you have a development of consciousness regarding the security of data, how to be aware, what you do, what you don’t, and that’s helpful. Then we have an insurance if something goes wrong.

Q: You mentioned you only had 3 options to get the insurance for companies like yours, so you do see a difference between the products offered to SMEs and the products offered for big companies?

R: Yes

Q: You also mentioned your information was put in the cloud, this is one of the reasons to get a cyber insurance, GDPR is another. Do you have more reasons? [Q2]

R: One of the reasons already mentioned is that all we have is our reputation. As an accountant the only thing we have is trust. If anything happens to us that undermine the trust on us is a damage, so you have to prevent that anything happens and one of the ways to prevent is to be aware. One of the things we implemented by having this insurance is awareness. It starts in ICT but it involves every person that works here. The main reason is that because we are built on trust, we could lose our reputation.

Q: You mentioned the IT manager, I’m wondering if your role has also to do with keeping the company secure of cyber threats, so are you responsible if an attack occurs? [Q4]

R: Yes

Q: You said the broker approached one year ago, before this, did you already know about cyber insurance? [Q5]

R: I was aware of cyber security. Before I worked here I was in medical companies, and there it was also one of the things that were discussed because the personal information about patients was one of the things they need to protect, and this is vulnerable information. It’s the same thing as we have here, information about clients, about patients, and to be a victim of an attack, ransomware and all those kinds of things, I was aware of that and when I came here I discussed it before I was approached by the broker. Because there has been an incident here, I don’t know the details, that was [SOME YEARS] before I came in, so they were aware of the threats and dangers. Then, when we talked about it, it wasn’t like I had to convince people.

Q: But, did you actually know there was an insurance for these kinds of threats?

R: No, I didn’t. I know that you can insure for anything you would like, but I wasn’t aware there was this specific insurance. I also thought it was part of the liability insurance but then I was approached, and the broker said it wasn’t the case, that I needed a special product.

Q: Q6. Do you know companies who already have a cyber insurance?

R: Yes

Q: Q7. What was their opinion about cyber insurance?

R: I discussed it with the owners because we are part of several alliances with other companies likewise that are in the same business, not competitors but that are in other regions. We approached them with this question, do you have this cyber security issues? What do you do about it? This is a sort of a union where there are big accountancy firms, then there is the group a bit smaller and this group has a sort of reunion where they discuss things, and they also give advice about insurances and all this kind of things. I approached the guy in charge of that, but he wasn’t aware of this, they were a bit ignorant. But we approached our member groups, and some of them had cyber insurance and some of them not. Of the 5 we talked to, 3 of them were aware didn’t have a product for cyber insurance.

Q: Q8. Do you personally know a company that has suffered a cyber attack?

R: I don’t know, they didn’t mention.

Q: Q9. What factors make or could make the company more susceptible to security attacks? Meaning, what makes your company easily affected by attackers?

R: The main reason why we wanted an insurance is the same reason why we can’t afford to lose the trust of our clients, and that’s also a reason for somebody to attack us or take advantage of our vulnerability, because they know that’s the only thing we have, then if they (the attackers) can compromise that, we have to do something because that’s the vulnerability we have, we build on trust. If we lose this we’re done, we can’t do anything. If the [CLIENTS’ PERSONAL INFORMATION] get published by somebody else, then other clients would think that’s not good and they would switch to another company, and we can’t do anything about it. So we have to be very precise about this.

Q: Where do you think most probably an attack will come from? Competitors?

R: I don’t think competitors, they are not a threat and the market is not that competitive. It’s more from people that are criminals. I lived abroad and what I saw is that you make your security better than your neighbor’s, the thieves would go to your neighbors, not you. That’s what we have to do as well, we have to build a wall that’s higher than our neighbor’s so they won’t come to us but to our neighbor. Criminals are there and if you don’t do anything or are vulnerable then you’re not aware. You have a risk, they will look for your weak point and harm you, that’s why we have to be alert, conscious about the risks and the trust we got from our clients. The threat is from the outside that is looking for an entrance opportunity, a weak spot. That can come from all over the world because we are in the cloud, we are very dependent on our supplier that is offering this service in the cloud, so they are also in the discussions about cyber security with us.

Q: Q10. Do you have alternative protective measures besides cyber insurance? E.g. IT security measures (firewall, intrusion detection system, antivirus), business contingency plan or company’s security policy

R: Yes, that’s what we have discussed with our cloud supplier, it’s a company advising us what to implement and what to control, be in the forefront of what is possible, and this goes for firewalls and this kind of things, to be able to defend ourselves.

Q: [Q11 and Q12 were skipped because the potential security threats were already mentioned (like ransomware and criminals trying to attack the company)]

Q: Q13. Is any of the next reasons a potential cause for you to not select a cyber insurance?

* Do not get a cyber insurance until other companies do so.
* There are no sanctions for not having a cyber insurance.
* Do not buy cyber insurance to save budget.
* It is not included in the security guidelines of the company.
* You think it is not necessary.

Can you think of any additional reason?

R: The main reason is that if you have had an attack they won’t insure you within a year or something. Then, after they had an attack (the company) they were aware that it was good to be insured, but they had to wait, and also because we were in an odd situation where we wanted to wait for this migration to the cloud and we had a supplier who helped us to be aware, to know the state of the art regarding firewalls and all this kind of things. So, they didn’t do it because, in an odd situation, we wanted but we couldn’t, and we had to implement ways to be in control.

Q: This security controls came from the cloud supplier?

R: Yes.

Q: Q14. But also the insurance is requesting you additional controls?

R: Yes

Q: Besides the firewalls and backups, do you remember additional security controls that were requested in order to be insured?

R: That your screen has to be blackout after a certain time, so if you leave your desktop it needs to be locked within some time, that was implemented and everybody was instructed that they needed to have this lock. That’s one of the main risks you have because somebody can do wrong things on your computer. Another thing we are implementing now is that people can work from home on their laptops and phones, but we have to secure the ways they can get access because it’s all about access. We are conscious of these ways to get access to be very strict.

Q: Do you use a private network?

R: Yes, if you want to work from home and enter the cloud, you have to identify yourself through an app that gives you a code, then you use this code to access the cloud. There are several checkpoints and security. That’s what we are implementing when you want to use the data in your phone as well, to have security checks.

Q: I’m also wondering if when you were in conversations with the broker did they say “you need to have this in order for us to insure you”?

R: No

Q: Just additional things like recommendations?

R: Yes, that’s what they did. They didn’t have real hard requirements. I use their requirements and advice to bring the awareness to the company because they also gave advice on how to implement security measures. That’s what I discussed with the IT manager.

Q: Q16. So, there was this attack before you arrived, was there another attack since then?

R: No.

Q: Q17. Do you know how the company dealt with it at that moment?

R: I don’t know the details but what I remember from the IT manager is that we were closed, I think, for [SEVERAL DAYS]. There was panic because they didn’t know what to do. I’m not totally sure but they had a problem, they solved it and then they could go back to work. From there, there was an alert of what an impact for not being able to work for [SEVERAL DAYS]. Since then we’ve had problems with the power here in [CITY] because of people working on the roads and they cut the power. Before we went on the cloud, the server park is here in [CITY], it has a backup power supply but that’s only for an hour to switch over to another power supply, but that also showed our vulnerability. This is another type of vulnerability but now that we are in the cloud, if the power goes out we can switch over to [BIG CITY], or even go to work to any other place with Wi-Fi connection. Prevention is always the best.

Q: Q18. Are the terms and conditions clear for you?

R: At the moment I convinced the owners of this security insurance, I was aware of all the details, if you ask me now, this happened half a year ago, so I don’t know them exactly anymore. At the moment I said yes, I understood them, since then I have to refresh it. This is a good reminder by the way because I have to sit down with my IT manager to make a cyber security plan about what happens if we have an attack, what would we do and also prevent as much as possible, but if the case comes we need to know which number to call so they can help us, this is one of the perks of this insurance because they can give you an advice, “don’t do this, do that, we take over, we will help you”. This is one of the things covered, a 24/7 assistance where a person will give advice, in some cases they will come over and help you out, they will do the negotiation, advice you what to do. The coverage of what and when I knew it, but at the moment has dropped, it has been some months. Also, I need to make the plan with my IT manager because he was also involved.

Q: Q19. What potential drawbacks would you associate with adopting a cyber insurance?

R: The only drawback I can imagine is that because we now have an insurance we will be less aware or think that everything is taking care of. That might be a drawback, but as I mentioned, we have an insurance now and I’ve asked my IT manager to make a plan. But we have an insurance and he might now think that the insurer will come. The drawback would be to think that the protection has been paid for, so everything is ok now and we can sit back and relax. I don’t want this to happen but it’s a possibility.

Q: Q20. What do you think about the premium price?

R: I think it’s fair. You take the decision of what’s the risk we take, and can we afford to be not insured. For our latest insurance, we had the same decision-making process. The insurance is to use it when our employees are sick for more time than a certain period to get money back from the insurance when this happens. We had to consider that we have around [COMPANY SIZE: 100-150] people. How many could get sick? What’s the risk? What’s the price? And then you decide upon it. It was the same with this insurance. We have a risk if we are shut down by a ransomware or by criminals. We could get out of business and this is a big risk. Then can we afford that? And no, we can’t. It’s a hard decision but we discussed it with the owners and at the moment the price is fair.

Q: Q21. How would you assess the success of the use of a cyber insurance?

R: That’s hard to say because we haven’t had any experience with the services they offer because we haven’t had an attack or a bridge of security yet. We only pay the price, we haven’t got any services back. Is the same as with the fire insurance, is better to not have a fire because you would have to start all over again, they can’t rebuild the building exactly as it is. Is the same with cyber security, is the premium, a price you pay because you don’t want it to happen. Is hard to assess what you get for what you pay because we haven’t got anything.

Q: Is the insurance renew every year?

R: Yes, I think it’s every year or more, but it’s renewable. So, at some point we could say no, we won’t continue.

Q: During that time, you might be approached by another broker, been offered something different, then it will come a time for you to analyze this.

R: Yes