Q: [GQ1] In which sector does your organization belong?

R: Financial service provider.

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

R: [BETWEEN 50 AND 100 EMPLOYEES]

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

R: [FIRST INTEREVIEWEE] Risk manager. [SECOND INTERVIEWEE] Legal department.

Q: [GQ4] Is there someone (or a certain department) in charge of security management? And if so, which role does it have or what department is it?

R: The operations manager, but this is also something that is been developing. We have our own IT house, sort of saying, it’s a sharing service center. That also triggered the need for getting the cyber insurance. The operations manager has the responsibility.

Q: So, you´re in the process of acquiring a cyber insurance

R: Yes, but recently we made the decision that we want to have it.

Q: [Q1] Which are the main reasons for getting a cyber insurance?

R: Many, first of all, the transition we are in, we are developing our own IT system, the awareness rose that we also have vulnerabilities in the digital surroundings and that we had to make arrangements to mitigate that risk. You get a lot of technical mitigation, mitigation in your organization with your employees, but that is not enough if you see the literature, the research, and the recent incidents, the cyber attacks on the news are increasing. On a global scale they are feasible but for our country it started to be on the agenda of risk and legal in the last few years, this is because of the responsibility our directors have. These were the main triggers to look at this mitigation.

Q: Is the transition an internal thing that is happening or does it have another reason?

R: Just internal rearrangement.

Q: [Q2] Are you working directly with the broker?

R: Yes

Q: Have you worked with them before?

R: Yes, they manage all our insurances.

Q: Were they the ones who brought up the topic?

R: Yes, it’s true.

Q: How long ago was this?

R: Almost a year ago.

Q: [Q3] One year ago, they brought up the topic about the existing threats, the insurance?

R: The cyber risk was already in our agenda, but that was managed by our shared service center, now we are bringing that in, so we have to manage it. Our broker suggested the possibility to think about the cyber insurance. At first, we were wondering what is it, why do we need it? Because we got all kinds of mitigation measures in place, but as you talk about the subject and learn more about it, and once is on the table, you realize what a big effect it could have in the organization. Mainly reputational. Then, that is something you can’t deny anymore. We made a memo to really get focused on it, to force the decision at the management level.

Q: Regarding the process with the broker, have you found any problems? Has it been difficult to understand the product?

R: No, it’s more difficult to convince that we need the product.

Q: Not with the broker?

R: No, but the impact is huge and the chance that it occurs is minimal, nobody has seen it yet. We only have the news and examples you hear from colleagues. The impact is hard to quantify to really get the message to the other side, that’s really difficult. You really have to make it understandable and that takes a lot of effort. Yes, and the chance that it will occur will be bigger and bigger in time, and the DDoS attacks just take a few months, they helped us convincing the managers.

Q: [Q5] Expanding a little bit on this. You don’t know directly any company that has had cyber attacks?

R: I was at several presentations where we heard a lot of DDoS attacks, but not personally. So, it wasn’t only in the news but also in the presentations and we heard from experts.

Q: [Q4] The broker was the first one who brought the cyber insurance topic to the table, but, did you know about cyber insurance before?

R: No (answer from both). That was the moment that we started to look at it as a mitigation possibility. That´s very strange, to combine these two together, the risk and the insurance. That image has to be filled when you build the expectations of the product, that´s where the energy went in.

Q: [Q6] When you were in these presentations, did you approached the persons/companies that mentioned they have had cyber attacks to know how was it and what happened?

R: Yes.

Q: [Q7] What factors make or could make the company more susceptible to security attacks?

R: Phishing mails, human errors.

Q: Something specific about the business or the type of data that you handle?

R: Yes, the financial industry is often the victim of cybercrime, and we have personal information of people. The financial industry is in the picture.

Q: [Q8] Which another type of alternative protective measures besides cyber insurance do you have?

R: An alternative for the cyber insurance? The quickest answer is no, none. On the other hand, we have technical measures in place, in the IT system, we have soft controls within the organization, with the employees, like the occasion when you want to log in at home, we have the badges/cards to get in the building, we have authorizations within the organization along with your functions. But, when something really goes wrong, you need a person to coordinate all the different kind of measures, that they are working properly. You have to inform the stakeholders, think about the legal implications, communicate with the press, check the reputational effects, and that is a role which we don’t have. That’s not our niche of expertise. That was the unique selling point of the product, to have that person with experience, 24/7 available, that can coordinate the process, who will guide us. With this, everyone can do their own thing. At least that’s what they promised us, but hopefully we’ll never have an incident. But, from the defense perspective, we can say that we have thought about it and that we have this measure in place. You have to do everything to mitigate as much as possible but is not a guarantee that you will not have any damage at all.

Especially for our business, we deal with public money, that makes an extra point for the reason we wanted to buy the cyber policy, for the reputation of the Dutch public sector.

Q: The company is not public, right?

R: No, we are a private company, but we deal with [PUBLIC SECTOR]. [NAMED SEVERAL CLIENTS]. So, is not only our risk, our reputation, is also the risk of the political figures behind that funding. You have to be upright. Is like a public-private organization.

Q: Did you talk to [ORGANIZATIONS] you work with about this?

R: No

Q: Did they give some kind of advice?

R: No. But looking in the nearest future these questions will pop up. Good risk managers are looking a bit further to see what’s happening in half year or the next year. When we have our own IT system in place, SAS solutions in the cloud, you have to deal with that risk. You should have a story to tell about how we manage that. The public sector is usually a bit later than the private sector, but eventually they will be there.

Q: [Q9 and 10] We talked about reputation, the human errors (phishing emails), you deal with public money. These are the security threats you see that might happen in the company. Which are the most important for you?

R: Reputation is the most important one.

Q: [Q11] What were the reasons for you to not select a cyber insurance?

R: We had doubts about the process.

Q: What about the price?

R: Yes, price. Also, that we have to manage it in our own, that other companies don’t have it and we do.

Q: Because you think it’s not necessary?

R: Yes, we thought that. I think it’s more related to the awareness. Another reason is that it almost doesn’t occur. The impact is huge but the chance is unlikely. We are just a small company and cybercrime will not pick us as their main objective. But that’s not the way the cyber world is developing. These were the topics that made us doubt, and the decision-making process was quite intensive.

Q: You mean the internal process with the directors?

R: Yes.

Q: [Q12] Has the broker requested to implement certain/additional security controls?

R: We have an appointment with them on [DATE AFTER THE INTERVIEW] where we will speak about these items, then we have to fill in all kind of papers for the acceptance of the insurance. So we are at the beginning of the process.

Q: So you still don’t know what they will be asking you?

R: No

Q: [Q13] What expectations do you have if you decide to get a cyber insurance?

R: They will take away the sorrow from us. Just in case, that’s what insurances are for. It’s a safety measure. The expectation is that they will take care of everything when having a cyber incident, if the impact is very big and we are not able to handle it, we have the option for calling the CISO [they meant security service provider], the case manager sort of saying, who will take the lead. We can manage a lot of things on our own but is really good to have that safety net. If you look at the price… I mean, I don’t know yet the gaps as Jaqueline was telling of the things we need to do before the insurance will really start… but the price is not something that will stop us.

Q: The premium price?

R: It’s peanuts, I think.

Q: [Q14] Has the company suffered a cyber-attack?

R: Not that we are aware of. Perhaps long before us, but I don’t know.

Q: I’m wondering that in case that it did happen, that could be a point of decision for the directors to go for the cyber insurance.

R: No.

Q: [Q15] Do you fully understand the coverage offered by your cyber insurance and in which cases you would be able to use it? Do you already have these details?

R: Yes, we know roughly the parameters. There are some financial damages, but the main value of the insurance is the service, that they are handling the incident, and the reporting, just covering all the facets of the incident. If there are damages, I think the coverage is up to [AROUND €2 MILLIONS].

Q: And the time to respond?

R: Yes, that is important. Within 5 hours of reporting

Q: Are you the ones who have to let them know that something is happening? Do they have some kind of monitoring?

R: I don’t know. I think we have to inform them. Yes, because all the contact with the insurance is legal. We have our own incident management system and when something occurs we can inform each other very quickly, and when there is an incident like cyber, our partner will be directly informed. It’s handy if the legal department does that job.

Q: [Q16] What potential drawbacks would you associate with adopting a cyber insurance? Like, the security awareness could go down?

R: I don’t expect that. I don’t even think people know that we have such an insurance. It’s a management decision, nobody has to know in detail the coverage we have with the insurance. But if they know, it could have an effect on the awareness level or the way people behave. But it’s also about the importance we give by buying an insurance, so we could also expect that people’s awareness will be higher, not lower.

Q: Q17 was already answered for their opinion about premium price.

Q: Do you have any plans for creating education programs for the employees?

R: Yes, that’s already in place but we’ll give more attention.

Q: Relating the process for getting the cyber insurance with getting any other insurance, what are the main differences that you can see?

R: There are not many insurance companies offering cyber insurance in The Netherlands. We trust our broker, they have a lot of insurances and they developed their own product in collaboration with the insurance company. We didn’t do much research for the other companies (brokers) offering the same product.

Q: So, mainly would it be the number of offers available in the market for this type of products?

R: Yes