Q: [GQ1] Which is your role in the company?

R: [RESPONSIBLE FOR INFORMATION EXCHANGE].

Q: [GQ2] In which sector does your organization belong?

R: [DISCUSSION OF THE SECTOR] The company is an IT company with knowledge of supply chain and logistics.

Q: [GQ3] What is the number of employees working for the company?

R: [BETWEEN 20 and 50 EMPLOYEES]

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

R: That is my responsibility. The major part of the platform is within my responsibility, but we don’t have it separated as it used to be, where I was responsible for the commercial platform but also for the enterprise, there is a colleague in charge of the PCs, the office and so on. [DISCUSSION of BUSINESS ALLOCATION]

Q: [Q4] Can we say that even that there is no department dedicated to IT security, this is something within your activities?

R: Yes, I’m still the security officer for that matter.

Q: So, you decided to have an insurance or are you still in the process?

R: We had an insurance when I started working here, like [SEVERAL] years ago, but the…

Q: Was that a cyber insurance or a different one?

R: It was like an economic insurance, liability. But the cyber insurance is current because of the ways the platform behaves with our customers, our customers with the growing functionality are put in the platform, the customers become more dependent with our services than they were 5 or 10 years ago. So, we have to be better insured for liability but also for cyber attacks and cyber damages, that’s why we considered the insurance and the discussion was started by [INSURANCE BROKER]. All our insurances go by [INSURANCE BROKER].

Q: How long ago did you start talking with [INSURANCE BROKER] about this product?

R: [ABOUT 3 YEARS AGO].

Q: [Q1] Have you worked with [INSURANCE BROKER] before?

R: This company has worked with [INSURANCE BROKER] for the rest of the insurances, not me personally.

Q: [Q2] Which are the main reasons for getting a cyber insurance?

R: It is the growing awareness of our vulnerability in that area, our vulnerability to cyber attacks, the consequences it would have for the company but also for the community. We had to make sure we have measures to rebuild if we are attacked. We are a small company, have a small budget, so we have to have insurances in case of something bad happens.

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

R: As I mentioned, it started by [INSURANCE BROKER], they gave us information about the insurance, the benefits, and costs. We had a discussion in my business area (the previous one as the former IT director), with our quality insurance officer, I discussed the benefits and the costs. With that proposal we went to the management team and there is where the decision was made.

Q: Was it an easy process between [INSURANCE BROKER] and you?

R: We decided within 3 meetings with [INSURANCE BROKER]. Very easy process.

Q: [Q5] How did you first hear about cyber insurance?

R: By [INSURANCE BROKER].

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

R: No, this is the first company I have worked with that has this cyber security measure.

Q: Or other clients mentioning that have a cyber insurance?

R: No

Q: [Q8] Do you know if other companies have had a cyber attack?

R: Yes. I participate in the [DOMAIN] ISAC, by the NCSC (National Cyber Security Centrum). They support several ISACs, the Information, Sharing and Analysis Centers, which are set up for all major industries like banking, water management, [NAMED OTHER SPECIFIC DOMAINS AND AREAS]. It’s a group in which confidential information is shared about cyber security, cyber attacks, and so on. There we also discuss the vulnerabilities for companies here in [AREA] concerning cyber issues.

Q: Is that how you got to know about the company having problems, cyber attacks and alike?

R: Yes. But also, the international problems.

Q: Yes, I guess when working with [LOGISTICS AREA 1] and [LOGISTICS AREA 2] you get to know a lot about international impact.

R: Yes, like the famous one that started in Ukraine, it led to the closure of one of the handlers here for two months. The companies who work at [LOGISTICS AREA 1] are the same companies that work at [LOGISTICS AREA 2], so there’s always a risk of contaminations, but we managed to survive.

Q: [Q9] What factors make or could make the company more susceptible to security attacks?

R: From a technical point of view, we have a lot of legacy systems, we manage them actively. As far as we know we haven’t had any attacks. Also, I don’t think we are that interesting to be hacked. From an organizational point of view, we are a very small organization, so we don’t have many specialists who can provide cybersecurity measures, and I have to admit that awareness, from a Dutch point of view, is very low. People are not aware of the threats and risks of how people try to gain information about our security, systems or platform.

Q: Because of these reasons, do you think that someone could easily attack you?

R: Yes, that’s an option. For instance, we’ve had fraud mail that people don’t recognize at first sight, we have to transfer the money and they have a nice bank account, then we realize that those email addresses don’t match, there is something wrong.

Q: Do you think that the information your company deals with is of interest for someone to attack you?

R: No, I don’t think that’s of interest. It’s only of interest if you want commercial information about your competitors, but the data we process is not relevant. It’s about shipments, and [MOST] of the information we have is publicly available and no party would be threatened by. Commercial information like booking, fees that are paid that could be of interest, we don’t have that kind of information.

Q: [Q10] Do you have alternative protective measures besides cyber insurance?

R: As I said, I’m participating in the ISAC group, that’s where we create audience about how to increase the security, it all starts with awareness. In [LOGISTICS AREA] it has also started [NAME OF CYBERSECURITY GROUP], the cybersecurity group, in which I participate as well, there we are starting an awareness campaign that I can also use with my colleagues because I think that’s where it all starts. Secondly, for the technical measures, fortunately, I have one of those geeks who think it’s very interesting reading all about it and implementing the latest features, so I think in a technical level we have good measures.

Q: I guess you have the common features like antivirus, firewalls, patches?

R: Yes

Q: Are there any contingency plans in place?

R: That’s one of the points of improvement. If the production site is out of order, we don’t have the measures in place to be up and running very quickly.

Q: So, in case something happens, decisions would have to be made at the moment?

R: Yes, we’re missing a script, hardware, backup connections.

Q: But, technically you have different security measures in place?

R: The center is in [LOGISTICS AREA] so if something happens the main damage would be there than to companies like ours.

Q: [Q11] We’ve talked about the potential damages of phishing emails and stuff like that, another type of security threats for which you wanted to get a cyber insurance?

R: The availability of the platform is the major one, we support 24/7 businesses here in [LOGISTICS AREA], so our services need to be up and running. Also, the increased dependency of the community in our platform, which means that our downtime we can have is decreasing, there are some emergency protocols provided by customers where we state that in case information can’t be provided digitally it will be done with manual forms, but the analogue way of working takes more time, the delay and processing of data grow, and downtime is only permitted for a maximum of [SEVERAL] days. That also means for us that we can only be down for [SEVERAL] days. That’s one of the constraints we have in our business, after that customers will be finding the companies in our community, which will be sent to us as well.

Q: [Q13] Before getting the cyber insurance, where there any reasons for you to think that you didn’t need it?

R: This platform we have now has been up and running for [ABOUT 20] years, and in those [ABOUT 20] years we haven’t had any incident. So, there were no actual reasons for having it. That’s always difficult in cyber, is an insurance, and every cyber measure is an insurance, and the cost versus the benefit is always a difficult discussion even in this company. That’s the main reason for not having an insurance or not having all the measures you could have.

Q: Could you name it as; the insurance is not necessary because this platform has been working perfectly?

R: Yes, we have had no pain.

Q: Do you also think that the fact that other companies or clients you work with don’t have a cyber insurance is a reason?

R: No, we don’t let us be guided by our customers in that way. But, [MAJOR CUSTOMER] and the government have demands on this area, and they want to know which measures we have, which insurances, which preventive measures, how to rebuild after having an incident. Our customers are growing and they have more requirements we have to fulfill if we want to stay in business with these customers.

Q: But they do not demand you to have this insurance, right?

R: The insurance has never been demanded, they only ask which kind of measures we have in place and, mainly technical and organizational aspects. An insurance is not interesting for our customers because they want to know, will it work? And if it fails, will it work again? The way we’re going to do it, they don’t care.

Q: [Q14] Did the insurer request to implement additional security controls?

R: I’m not sure, I think there were some requirements, but I don’t really remember. There was no check from the insurance company or [INSURANCE BROKER] on which measures we already have in place.

Q: [INSURANCE BROKER] also works with some IT companies that can give support, is this the case?

R: No, not in our case.

Q: [Q15] What are your current expectations with your cyber insurance policy?

R: My expectations are that we will never have to use it.

Q: [Q16] You mentioned you’ve never had a cyber attack, right?

R: Not that I know.

Q: [Q18] Do you fully understand the coverage provided by your cyber insurance and in which cases you would be able to use it?

R: I think it was pretty straightforward and easy to understand.

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

R: No, only the cost.

Q: [Q20] Do you think the premium is high?

R: I think it’s fair, otherwise we wouldn’t have taken it.

Q: [Q21] If there is something to make you say I’m stopping this insurance, or I’m changing, or I need to reconsider or renegotiate, how would you do it?

R: The way we build our current platform is that everything in the data center is our own, our services, our hardware, our software, we haven’t outsourced this. What we are doing now is that we are renewing it, building a new architecture, which uses more cloud services. So, the balance between what we have on our own property versus what we use as a service might change the requirements we have on cyber security. We might make agreements on cyber attacks, what to do with that? Which party is going to pay? Who is going to be liable for the cyber attacks?

Q: Now that GDPR has come in place, does that has something to do with your decision?

R: Not at all, we’ve had the cyber insurance before the deadline.