[Before starting the interview interviewee explained a bit about the liability insurance they have] [We are insured for some liability from our customers no matter how it happened. If the impact is impacting our customers to a certain extent we take the liability no matter the factor of the problem; if someone is stealing something or a cyber breach. So is not specific cyber insurance, it’s more general liability insurance that includes cyber to some extent but is very hard to get coverage for cyber.]

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

R: Security defense IT, whatever categorization is best for that.

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

R: [BETWEEN 50 AND 100].

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

R: I’m the CEO and one of the shareholders.

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

R: There are three parts. We have an application security capability that takes care of the security of our product. Then we have a corporate security capability which takes care of the security of our house. We might do something very special for our customers, but I say those two are the primary. So corporate security and product security.

Q: Regarding the liability insurance, with what kind of broker or insurer are you working with? Are there national, global?

R: We have one broker here in the Netherlands that works with insurers here and in the States. That’s the only two places where we have specialized cover.

Q: Is geographical coverage what you have?

R: Yes. We have one global coverage but is done from the Netherlands, from the Dutch Law. Then, we have one in the U.S., specifically for the U.S. because is treated very differently. Most global insurers will not cover the U.S. for most things, so we have to have a very specific insurance from a U.S. insurer, that is more expensive.

Q: Do you do that because you have clients in the U.S.?

R: Yes, our clients are global. We don’t have Dutch clients so much, most of our clients are literally scattered across countries, and our people is scattered here, in London and the U.S.

Q: What is the reason for also having the coverage for the U.S.?

R: We have a U.S. entity that takes on U.S. liability, and for customers that are international companies like [MAJOR CLIENT], they have a large operation in the U.S., and there is a risk of liability because they do, no matter if we have an entity.

Q: [Q1] Could you explain why do you have this type of liability insurance and not cyber insurance?

R: The responsibilities of our customers are in the exchange of software and the exchange of services. In the case where there is an exchange of software they use the software that we create to perform a certain job, then we have to warrant them things like it works as intended, it does not have a backdoor in it, and we try to limit the time the liability they can come back on us by them using the software to the maximum extent. For example, they might say, if we have damages as the result of using your software is your responsibility. We say no, that’s not normal if you miss supplier software. All these rules dictate how they should use the software and under what conditions we have liability, but those conditions are usually around things wrong with our software resulting in damage, or us knowing and not telling them about there is something wrong in the software, so we insure ourselves for that impact. That impact can be created in many different ways. It can be created because we did something wrong, because an employee builds something in the software that he shouldn’t have, because somebody hacked us, maybe something in the software. So, I’m only insuring on the impact, and what we are saying is no matter what happens, I would like to insure general liability as a result of these contracts we have with our clients.

Q: Does that happen in a contract by contract basis or is it a general practice that you’re implementing?

R: Our insurance is general. However, the maximum liability cap that our customers demand from us is much higher than the ability for us as an SME to get that amount. There is a gap that is a risk for this company because the insurance would not want to insure us above a certain amount, and our customers demand us to have a much higher liability gap than the insurance want to give us. That’s a risk we are taking. And this is because we are an SME, that´s a negative effect of being a small company.

Q: How long has the company been operating?

R: [ABOUT 5 YEARS]

Q: How has being the process for getting this type of liability insurances? Did you ask for it? Like asking coverage for the impact instead of the losses? Does the broker provide this, or do you ask for it?

R: We asked for it, although is a standard type of insurance, is kind of general liability.

Q: [Q2] But some general liability insurances do not cover cyber risks. How are you sure that you are protected from those risks?

R: Clear. First, we have our legal counsel. We have a full-time lawyer working here just on this kind of liability issues, among other things. The role of the corporate lawyer is to manage the liability of the company through contracts. We were able to be very specific in asking for liability coverage in certain conditions, for certain reasons, in these countries, these geographies, and so on.

Q: So, the lawyers go to the brokers and start making these arrangements?

R: Exactly. But, it is very hard to get coverage for everything, simply because one, we are a small company and two, our customers are very big, and potential future impact can be significant, and three, it is true that most insurances do not know to estimate the likelihood most of the things related to cyber really. Their ability to price something that is affordable without being specialized is very hard.

Q: Did you talk to some of the insurance companies that provide cyber insurance to know what they offer?

R: Not exactly what they offer, but at least the broker in the U.S. was one of the few that had this in the portfolio.

Q: Did you consider that what they offer was not enough?

R: They are on the safe side, even that we are a small company.

Q: Was that with the broker from the U.S.?

R: Yes. Because is not about a standard, small ransomware or small breach kind of impact. It´s a multi-billion-dollar potential impact. So, they would overestimate the likelihood in our view and therefore charge us a significant amount of money, something we are not able or wanting to do. That´s still a problem.

Q: Is your role in the company related to keeping it safe from cyber attacks?

R: In the end everything is my responsibility but is a special interest to us because we work with [GOVERNMENTAL SECTOR].

Q: Is it also because part of your activities are related to identifying these risks?

R: Exactly

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

R: It was a long time ago, 13 years ago maybe. There were two big U.S. banks that starter to research how to provide coverage for cyber incidents, and our company was one of the first to provide them with the information they needed to make those calculations. That’s the first time personally I have been involved in it but from a different angle.

Q: Did they ask you to provide these calculations or were you already offering these?

R: The product was already offered to them in general. So, our customers were large [FINANCIAL AND GOVERNMENTAL ORGANIZATIONS] to know the threat landscape so they know how to protect themselves. The extension of that was realizing they could use that for insurance.

Q: So, they wanted to apply this knowledge to a different product?

R: Exactly.

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

R: I’m presuming so, but knowing for sure, no.

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

R: Thousands, yes. It’s our business. Our clients are having breaches every week, every day. You have the time before something happens, the breach, and time after something happens. Before, they use our software and our services to know who can potentially attack them, and when something happens they use our services to identify who and why, with what means they were attacked.

Q: Ok. I understood that your role is only involved previous the breach.

R: Usually, we’re only pre, so we don’t do the response ourselves, that’s for other companies. We deliver the intelligence that they require to make the response. For example, a [SECURITY SERVICE PROVIDER] would go and respond as a responder, they can potentially use our intelligence to determine what it was. We don’t do the investigation.

Q: From your experience with companies suffering cyber attacks, what are the main implications that you have seen?

R: Pretty much everything. We have seen process disruption when things slow down or stop working. From an impact perspective, we’ve seen monetary theft, assets outflow, things like someone stealing CO2 emission certificates. We have seen intellectual property theft, not detected immediately, it took some time because is something you copy not steal, so it’s harder to identify. We have seen physical threat, specially hacktivism and activism style. Think about oil companies were executives were under cyber attack, but the result was people feeling unsafe. When they’re at home they knew other people knew where they live. If they have children they know which school they go. Things like that. It’s very different kind of impact but a very real impact. Also, conceptually complicated, but as a result of espionage. If you lose information, if you´re a government or an oil company, about how and why you operate, you might lose negotiations for tenders. We´ve seen not information property loss but information loss. Or, cyber being uses as a mean to listen to conversations. Also, political influence, through extortion or other types of leverage that could be applied to people. So, I think we have seen must of the scale of potential impacts.

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

R: That´s a very hard question. The problem with cyber and the problem with insurances is about a balance. Security is not something where if you do these things you are secure. It is more a measure whom are you and it begins what are you trying to protect yourself, and you have to be proportionate on what you do. The biggest problem with cyber and for insurers is to determine what is proportional for a specific company. For example, if you want to protect yourself against espionage is so disproportionate that you can´t invest against it. Even a large bank, like an [MAJOR BANK], they give up as well. There is a level where they say we can´t protect ourselves against espionage. The capabilities of those adversaries subrogate for us to invest against. The reason why people get attacked is because one misjudges: what that line is, where they´re trying to protect against, and what risk is to accept. Then, there is a question of investing in and implementing the measures against those problems. So, there´s a problem where especially smaller companies don´t know what they´re up against. So, they also don´t know what to invest, and what they invest is driven by sales pitches, people not with the intent on protecting them but with the intent of driving revenue. For example, if you´re an SME and go to a small security company to ask for protection, those smaller companies don´t have the kind of knowledge to have this proportionality. So, they would sell some devices and some software, but they don´t know where they are in the ability to protect against what kind of problems. Bigger security companies can help other companies have both sides of the history: this is what you´re protecting against in this way, and this is what you´re not protected against. Therefore, you need to accept, or insure, or something like that. So, the biggest problem is the expertise. IT is not security and security is not intelligence, and nerds have a great ability to overestimate their capabilities and most smaller companies don´t have the expertise in security to implement things. There´s no point in integrating all the technical things that can go wrong, that´s infinite.

Q: Correct. According to your activities, your size and what you do, what should protect from?

R: There are different angles. We have the angle of our software, so we are protecting against anyone who wants to influence our software that operates in the [GOVERNMENTAL ORGANIZATIONS], this would be espionage related. It could be hacktivism or activism related, but their capabilities aren’t significant enough to make an impact. It also means not only espionage from this office, in the data centers, is also when we travel with laptops or phones to different countries, we have to be very careful. That’s one angle to protect against. Then there is a normal work corporation, so we have to protect ourselves against disruption, ransomware, financial theft and things like that. We have been targeted, and successfully targeted, but that’s more the problems everybody is facing and that’s fine. That’s another area, we call it junior-enterprise-IT-related problems because everyone who’s a junior can implement standard things that will be tried to be exploited. Then we have another one which is more competitive, that’s where you have industrial espionage or people trying to get access to what you know and what you do, why you do it and what are you going to do it in a few years.

Q: [Q7] Could you elaborate on the protective measures you have in place?

R: Starting with the generalities, you first need to create visibility. So, all of our laptops and servers they have a few different pieces of software that allow us to see what’s going on. Sure, it’s antivirus but it’s more monitoring of the activity on the laptop, and it goes to a company in the U.S. that validate and monitor everything that’s happening in the laptop. So, they would see if someone is reaching out to a website that is known for a certain virus or something to that extent. That happens in all of our servers. Then, we have social monitoring. Every employee has [SOCIAL NETWORKS ACCOUNTS], and we monitor their activities there, to determine if there are false identities. For example, we sometimes have somebody building a [PROFESSIONAL SOCIAL NETWORK] page with almost my name but not completely, but they use my actual image, so we detect my image has been used, which can eventually lead to people thinking they’re communicating with me. We have that for all the employees. Besides, in all the laptops we have encryption software, so when their stolen no one can see what’s inside. We have data segregation, so everybody only sees what they should see. Like customer information is only seen by certain people but not by engineers, the engineers can see the code but not by others, etc. When you go up, it gets more specific. Here is where there are specific government sales people or people like myself from the executive level. When we travel, we travel with empty laptops, with new phones, because we fly to the [EXAMPLES OF GOVERNMENTAL ORGANIZATIONS]. So, they will eventually do something with your laptop. We’re now starting to have spot check monitoring because we have a lot of information about cyber threats, to see if we can find any indications on laptops if something is wrong. Is more proactive to look into activities in our IT system to see if something is wrong. So, is not waiting for us to detect something. Is to know what would it look like if the [THREAT ACTOR] were here and tried to find it? But, I would still give us a six on this. We have a long way to be able to protect ourselves like a mature company could. Most of it because of the resources.

Q: Resources regarding people or the technology? Or is a combination?

R: All of it. You need people to have eyes to look at something, you need technology to have visibility and you need intelligence to know what you’re looking for. All those things are vastly expensive. If we wanted to give ourselves an eight, we would have to invest as much in security as we would do in our entire IT infrastructure, and we don’t have that money. But we are expected to accept liability for that regardless, that’s a struggle.

Q: Do you outsource part of your IT security?

R: We do. All the continuous monitoring happens elsewhere. The software is here, we do check ourselves, but the eyes that look at it are not here. Because we can’t staff someone that looks all the time. But we will. The next step is this office. We will move the office to a more secure location. To have locks and proper things so we can get a classification from the governments so that [TO INCREASE TRUST TO INTERVIEWEE’S COMPANY].

Q: [Q10] You have mentioned some reasons for not getting cyber insurance. Do you have other reasons?

R: One is that they would not give us enough coverage, so we would need a maximum of [ABOUT 10 MILLION], and they would not give us more than [SEVERAL MILLIONS]. Another one is the cost, we’ve seen is too expensive. Another one is our balance sheet. We are a company that is highly invested in, which means our revenue is smaller than our spent or cost. So, if we don’t invest in the company we would be making losses and that’s hard for insurers. They would like to see cash-positive and profit-making-companies so many insurers simply say we don’t want to insure you because you don’t look like a healthy financial company. They like to have later stage companies. Finally, is that they simply can’t cover certain things. They would not understand perhaps what we need, or we wouldn’t trust them. Not all insurers are cyber-aware enough, or the sales people aren’t. So, when you hear them describe what they would cover is not specific enough that it would actually work if something happens, then there would be a conflict and you would not trust them to understand what is happening.

Q: [Q12] You mentioned you suffered cyber attacks. How did you deal with it and what were the impacts on the company?

R: I think we are being attacked every day. The two or three successful examples are, one is financial. They were smart enough to understand who to mimic and who to pretend to be, they were using our templates, the impact was not so much, [ABOUT SEVERAL THOUSAND EUROS]. We spotted it a few minutes after and we knew how to respond to, it’s our job. The response team came in, put the forensics on it, we understood how it happened, we changed the controls that were around the process, we learn from it and evolved. The standard incident response came in to see where to begin and what to learn. Another example was espionage, people trying to get into our systems to understand how our software works. They didn’t get far enough, we were able to identify it quickly and respond to it. This is one of the examples were very advanced cyber threats use mechanisms that are unknown and there is no ability to protect yourself. There’s nothing you can invest and they can no longer do that, so you have to build multiple layers and things to make it complicated to them. This was a matter of making it even more complicated. There was nothing to be learned, we could not protect ourselves better than we could give this balance we are trying to maintain. The other examples were very simple standard stuff, a laptop getting infected by some ads, simple virus and that sort of things. There is a potential impact, they could have got access to our source code, but they didn’t, also because that’s not what they were after. They didn’t know about it, and they were just trying to do something automated.

Q: Yes. There are these two types of attacks you’ve had. One is specialized and the other is commoditized.

R: Yes, but we are not to bothered about the second one.

Q: Is it because you feel you're protected enough for those kinds of attacks?

R: That plus you will always have the impact from it as a business. Any business will always have that. It’s a matter of whether you can recover quickly.

Q: [Q11] What are the additional security measures you will want to implement?

R: I say more proactivity. Very specific looking for potential attackers on the network, because otherwise you are only aware of it when something breaks or is stolen, or when the detection software indicates something is happening. But if they get passed that, you never know. The rest is process control, we are a young company, which means we are not process heavy. Most of the controls that are implemented are the simple process like a new employee needs to get a pass for the door, if he goes away he needs to give it back. Or controls like what people get access to data.

Q: What kind of drawback do you think are related to having a cyber insurance? Some companies have mentioned that this type of product could potentially low the security level of the company because someone else would take care of. I don’t see that happening in this company.

R: I don’t think so, also because I doubt enough breath of impact can be cover by cyber to have that kind of behavior. Not all impacts are monetary and therefore, the ability of an insurance company to compensate you for that only applies in certain cases. Even if they would compensate you for a loss of productivity, or downtime or slowing the business, is still very disruptive. So, we would never start to be lazy in that regard. A drawback is definitely the price.

Q: [Q15] When you considered the premium prices for cyber insurance, was it only with the U.S broker?

R: Also, here, I don’t know which insurer was. For larger impacts is very expansive, simply because they can’t estimate the likelihood in general, for everybody. That makes it very hard to understand what measures the company should take so they can estimate how much they should ask for. Is not only about expertise, but standardization is also not there yet either to assess the company’s level of maturity. That’s a blocker for complex organizations been insured. Smaller companies could more easily insure itself because impacts are easier to understand and measures are easier to categorize. The more specific you can get it the better, if you’re a builder and you’re protecting yourself against laptops that have to be replaced because of ransomware or something like that, is a very easy use case, and easy to expect. There’s also a difference if you’re protecting impact in your company or if you’re protecting impact that you accept on behalf of your customers. That’s more our use case. If this company goes down, the cost of that is a fraction of one of my customers, so my interest lies somewhere else.

Q: Finally, when this type of decisions has to be made regarding the selection of the insurance, how is the process in the company? Are there specific persons in charge of taking the decisions? Does it take a long time?

R: Is mostly driven by the fact we have to be legally audit ready, which means you have certain controls in place. If that’s the case, it means that the CFO is accountable for those risks, and he is the one driving what impact should be insured in what way. In his team, he has his lawyer, finance team and so on. He is the primary driver behind it. My role in that is at the end, to see if the assessment is correct if it’s worth the cost and so on. Our board of directors might influence us if they ask questions about coverage for certain problems, but we haven’t got there yet. They wouldn’t have to decide, they would only give recommendations. If we wouldn’t have anything in order, maybe they would have already done it, but we do.