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

R: CEO

Q: How many years has been [COMPANY] operating?

R: We’re a venture capitalist funded [LESS THAN 5 YEARS AGO], we started as an open source project in [AROUND ONE YEAR BEFORE GETTING FUNDS].

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

R: Application security

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

R: [BETWEEN 1 and 10 EMPLOYEES]

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

R: That would be me, we are like [SEVERAL] developers specialized in security.

Q: Do you have IT security outsourced?

R: Nothing is outsourced

Q: [Q1] The company decided not to get a cyber insurance. Do you already have other types of insurances like E&O liability, professional liability?

R: I’m not sure what we have. We have insurances for employees, benefits and that sort of.

Q: Are the insurances you have the mandatory ones?

R: Yes

Q: [Q2] Are you aware that any of the insurances you have are not for covering cyber risks?

R: Indeed

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

R: We thought of it as selling our product to insurers to reduce the risk. Consider applying for insurances as a company but it didn’t make sense to go that way.

Q: About the product, did you read about it? Did someone tell you about it? How was your first approach?

R: We read about it or we talked about the opportunity that could be there for selling our product to insurers, as a channel.

Q: I’m thinking in the sense that, there are insurance companies offering cyber insurance. I want to know if someone approached to you because you are in an early stage company, and because of the work you do you need to protect your company against cyber attacks. I’m talking about cyber insurance in that context.

R: We think about it in two contexts. One is, if we are hacked we are probably out of business, so is really hard to insure that with the damages and the evaluation of the company. Insuring it doesn’t have a benefit. We have to implement all the measures to have a secure platform. We think that if we implement all those measures then we are really secure. Insuring does not benefit anymore.

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

R: I’m aware of none, yet.

[Q5 was not made due to previous answer, but still try to get more information about interviewee’s perspective regarding other companies and the use of cyber insurance]

Q: Do you think this is something companies are aware of?

R: I think companies are aware of that, and there are some challenges in buying those products from the commercial perspective, from the sales perspective. We’ve thought about selling our product to insurers so they can reduce the risk and the cost of the insurance. There are some few challenges, why would you not want to do that as a vendor? From the vendor perspective, for early stage companies, I think it will be really hard this to sell to an insure. For example, we can sell something to protect your applications from being breached and actually insurers are consumers of us, they have the product but not selling it. We can make sure that if you have an insurance portal you can securely develop it and then we protect it against hackers in real time, that makes sense. But if they sell a subscription for an insurance, they have to be very clear on what they cover and what they don’t cover. From the buyer perspective, if you buy an insurance you want it to cover everything, because what’s the point of being very specific? Very often the buyer doesn’t have all the knowledge on what they need to make a decision, so the seller will typically sell “we secure everything” and the buyer will ask “can we have everything?” and then, from the vendor perspective, from an early stage company perspective, we can never sell a very niche product to the insurer because the insurer has already sold everything. The risk for wrapped applications like ours, unless they perceive this huge risk, they will never buy from early stage vendor. That was for us a challenge.

A network security company sells a product, and additionally, they guarantee up to 1 million in liability if the network is compromised. They think that can work, and that works typically in later stage vendors, mature vendors. If they target late majority, these propositions make sense because at the end for a vendor is a cost. To convince the late majority, or a laggard in terms of adoption cycles, that works really well because these companies want to have finished products and finished propositions. They don’t care about the technology, so if you have the proposition that makes a lot of sense. We can sell it, for every hack we cover up to [SEVERAL MILLION] but our customers take care about the technologies and they don’t care about the rest. It’s only a cost for us and it doesn’t help with the proposition. It’s really important to see this adoption cycle and if you look at the seller of those subscriptions with the insurance policy, we know the market is very well defined because otherwise, you cannot exclude wrapped applications from the security because the buyer will always expect everything to be covered, or it should be clear. That was the main challenge.

Q: If an attack happens, financial losses are covered, but also what the buyer is asking is that they don’t only want the financial part to be covered, they also want legal advice or someone to deal with public relations and defend the image of the company. The insurers are trying to be careful on what they are providing, or they have to make security check controls in the company to know if they have a minimum of security in place.

R: Yes, and that might work, to reduce reputational damages by procuring lawyers, but you’re competing with big companies, consultancy companies are doing those services right now. It’s a cost saving at the end, from the buyer perspective. It would be hard to sell something like that.

Q: Do you discuss the topic with your team or also with others?

R: We discussed it with an insurer and we did some analysis but then we come back to the fact that it’s an additional cost, the insurers want to cover that if an application is hacked they will cover up to [SEVERAL MILLION], and we won’t do that because it’s a cost and does not help with the proposition. For the insurer is still an additional cost, for the buyer it should be a cost saving. So, we said, we don’t want to do this.

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

R: We analyze our customers’ data, we receive a lot of PII, that would be the biggest risk. We have emails, developers with laptops but you know, securing a developer laptop is challenging, so we have other measures in place to make sure that the code is secure, and we communicate in a secure way. For email, we outsource that, we use Google suite of applications, so the risk resides in Google.

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

R: We have encryption, we do intrusion detection. We typically host parts of the product for customers, so we take care of that. Then, we do intrusion detection. We have automated systems in place for authentication, and we do that centrally. For a sense of things, we do encryption. For consumer communication, if things are sensitive, we can set up an encrypted channel but, typically, consumers find it hard. So, in the end, it still relays on the cloud. We do this for ourselves, for clients we do intrusion detection.

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

R: That would be IP loss because we are part of an open source company and part of a closed source company if we lose that it would be a problem in terms of company valuation in an early stage, and perception of the product. Loss of PII data would be the biggest risk.

Q: Which type of attacks are the ones that could damage you the most?

R: We don’t think about it specifically, we have technical measures in place. Like, phishing could happen but it won’t have any big impact. With the technical measures in place, we make sure that the latest attacks cannot impact the company.

Q: [Q10] For you as a company, besides the fact that you have most of the protective measures in place, for what reason you would not get the cyber insurance?

R: The biggest risk for us is to be out of business after a breach. Even if the insurance covers legal costs or PR costs we would still be gone. There is no added value. We have to implement all the technical measures and if we do that I can say we are quite secure because we have all the security engineers working at our company so, by putting the same amount of effort in technical measures we cover it better than doing it with the insurance.

Q: For you having a cyber attack is the last thing that should happen

R: Yes

Q: [Q11] Do you think there are additional security controls that you can implement?

R: Right now, no, we are implementing all the controls.

Q: Do you know other companies that have been attacked?

R: Yes of course, many.

Q: What kind of effect have you seen for these companies?

R: We see reputation damage, make sense of course. We see that there is a cost in fines. The fitech breach was interesting because they were fined from the US government and the fine was because they said they implemented certain measures but it turned out they didn’t have any of those measures and the fine was bigger. Today we saw [PUBLIC ORGANIZATION 1] had a breach, they say [LESS THAN 10] records were stolen from the systems but the reputation damage is there and we are securing one of their competitors so that is interesting. Then you have the consequences in the technical implementation, so you have to now apply technical measures because you have to ensure this never happens again and while implementing those technical measures your teams cannot continue developing new features and they are more worried trying to solve this problem as fast as they can. Your organization is slowed down trying to finding out what happened and filling out the reports.

Q: What type of companies are the ones that are most attacked?

R: It’s hard to measure and distinguish it. The type of companies that typically buy our product are product companies, so that the company has one product, and that product is the company. A company like [PUBLIC ORGANIZATION 1] is sending employees over; one of their competitors have an online platform and if the online platform is down or hacked, the business is over. Or like payment service providers, for those type of companies is relevant, they act on a daily basis.

Q: So is it more on the activity?

R: Yes, but it changes as well because for instance [PUBLIC ORGANIZATION 2] is a consumer of ours and for [TYPE OF ORGANIZATION] everything is on the endpoint, and [DESCRIBED SENSITIVE INFORMATION]. Monitoring that closely is very important to them. So, it changes. Companies that used to have everything offline have it now online and accessible by everybody.

We have researched for [EDUCATIONAL ORGANIZATIONS] about what they perceived as a risk. We called every CISO or the responsible for that role and we asked, what is your perceived risk? And the students were very high on the list.

[Q12 was not mentioned since he had already mention they have not suffered a cyber attack. Q13 was not made since according to the previous answers, he does believe the company has a good security management strategy]

Q: [Q14] Is there something that would motivate you to get a cyber insurance?

R: No

Q: [Q15] Have you discussed the premium price?

R: No