Interview guide – IT Security consultant.

**Who are we?**

* This interview is being held as part of our course called Software Engineering, where our group, consisting of Cecilie, Luca, Peter, Victoria, and myself are tasked with managing an agile software development process where we develop a system based on a case. The case that we are investigating is an interactive assistant designed to help smaller businesses assess their IT security situation and use of technology in general and make suggestions.
* The outcome of this course is a low fidelity prototype, but the purpose of the course is to manage a software development process and show that we can deliver everything associated with that.
* The purpose of this interview is to discuss IT security in the context of a small business, to understand who the user of a system like this would be for.
* We are not to focus on the viability and the intricate engineering requirements of such a system, but rather play around with the thought of what the app could do.
* Any questions?

**Practicalities**

* The interview will be recorded with the intention of transcribing it and using it as an appendix in the final hand-in. Is that okay?
  + As part of this you will be anonymised.
* I will be taking notes during the interview.

**The informant presents themselves**

* Would you like to introduce yourself? Your name, work background and what you do now?
  + *Used to work within sales and management in the US*
  + *Moved on to the banking sector*
  + *Has been a part of two smaller companies.*
  + *Just finished working as an interim head of IT security in CIP.*
* Do you have any experience owning or being part of a small business?
  + *CEO of a small software company with 25 companies – which sold*
  + *Then CEO of 3-person company making equipment for sport. The company is alive and well and Peter is a board member.*
  + Can you tell us a bit about the IT aspects of the business, i.e., what systems/software were used?
    - *The big company (“sigma estimates”) - Back-end + CRM system was developed inhouse.*
    - *The Microsoft package.*
    - *Some American software to power the online shop.*
    - *Finance function outsourced, as was bookkeeping.*
    - *Marketing software by some provider.*
  + What did you consider in terms of IT security capabilities?
    - *Everything was cloud based – so responsibility fell on the service provider*
    - *Their own responsibility would be GDPR.*
    - *Establishing policies in terms of not storing stuff on their own laptops and using the cloud was the pretty much the extent of what they thought about.*
    - *Common sense in terms of awareness.*
    - *It’s a big investment to look at policies like ISO for small businesses.* *As long as what the customers use is adequately set up, small businesses don’t need to worry about these kinds of policies.*

**IT systems in a small business**

* The use of IT or an “IT setup” in small businesses can be very different depending on if it is just 1 person, 5 people, or 20+ people.
  + Could you help us understand how the IT setup differs from that of the smallest businesses compared to a bit larger one, and what they have in common?
    - *These companies have more in common now than in the past, with many easily manageable software products being on the market, which target both very small and somewhat small businesses who have the same business needs that need to be fulfilled.*
    - *But it largely depends on the offering of the company.*
      * *Hair salon example: They only offer a service that takes place physically without IT systems. IT supports the business in terms of bookings and handling money and customer data.*
      * *Software company: A businesses with another kind of offering, like a software product*
* What IT security capabilities are essential today?
  + In terms of regulations (privacy, data, etc.)
    - *Data protection is important to comply with any local regulations a business may have, but awareness is the most important generally. It may be more important for businesses with some sort of product offering, since they face other risks than for example, the hairdresser does.*
    - *It can be generalised as prevention, that prevention is the most important, in the form of awareness. Then, internal processes and policies that describe how to navigate IT internally, and how to react if there is an attack.*
  + *Internal processes need to be in place for what to do if adversaries ever get access to a business’ system.*
  + *Multi-factor authentication is not a requirement by any laws, but many businesses don’t see the importance of it, and how much harder it makes it for an adversary to access the company system.*

**External IT security threats**

* What are the main IT security threats that any small businesses face?
  + *The threats that a small company faces are much more different than those of a larger*
  + *Someone with malicious intent may not attack a hair salon because their data is not deemed that important by the business owner.*
  + *Phishing attacks may happen against hair salon owners and employees, but just the same as what happens for individuals.*
* Say that a business is using some software systems by a software provider. Are the small businesses responsible for preventing/dealing with malicious attacks or does the responsibility fall on the software provider?
  + *The software provider is responsible if their product that the business uses gets infiltrated.*

**Awareness**

* What is the most important aspect in terms of IT security?
  + When we spoke a couple of weeks ago about this case you mentioned that proper awareness training is one of the largest issues when businesses are faced with outside threats. Can you elaborate on this?
    - *As mentioned, having awareness training about concepts like phishing and social engineering is really important today, since a lot of attacks are done with these types of methods. Humans/employees are the weakest part of the IT security of a company.*
* Do you think that IT and IT security is a foreign topic for a lot of small business owners that results in them not knowing the importance of it?
* Do you believe that a better proficiency in IT will strengthen the business owners’ belief in their own IT capabilities?
* Do you think that awareness training should be a main focus of the system we are developing?  
  + *(Answer to the above questions):*   
    *Use some marketing that indicates that this can cause you money if you don’t look at awareness. Creditcard example. If their business Creditcard gets fraudulently accessed and they must deal with it, it takes time. Time is money and their money is important for a hairdresser.*

**The market**

* From our market research, we found that companies who provide software on security, compliance or awareness, usually only focus on one of these aspects, sometimes combining two, but not all three.
  + What is your opinion on making a solution that can “do it all”, versus one with a certain focus on one or two of the aspects? What is better?
  + *(I believe) Customers usually look for a piece of software that can either advise on security or compliance, therefore they are separated. But if the providers were to suddenly offer another branch of awareness in the existing software, then customers wouldn’t mind.*
* Would you know of any services/consultancies that assess and advise small businesses on this topic?
  + *No not really. In my current work we use consultant firms that have a different offering and target customer in terms of compliance and security.*

**Conclusion**

* Based on our talk, how would you define the target user for a system like the one we are “developing”?
  + *There can* *definitely be different types of customers, but they face different kinds of threats:*
    - *Smaller companies, like any civilian: credit card information can be stolen*
    - *Larger companies: corporate espionage, ransomware*
  + *The app should not be intrusive at all, as you wouldn’t want the business owners to think that this is a big undertaking that takes too much of their time to learn.*
  + *Gamify an app for small business and give them trophies for completing phishing tests issued by us.*
  + *Statistics should not be public to all employees in the company (this is with an example company of 10 people), since the “bad” performance of some employees should not be laid out. Rather, employees should instead want to talk about and brag that they have completed a new test successfully (phishing test for instance).*

**EG:**

* *EG has a software solution for hairdressers (+ a host of niche solutions for different businesses.*