# Transcription expert 3

Duration: 60 minutes

X: Could you explain to me what a VPN is?

Y: Yes, so you're gonna cold call me out. VPN, in essence, it stands for Virtual Private Network. So, it is a way of, of getting access to a private network. For instance, if you look at our company as [the professional services firm], to our, eh, corporate private network. And that way of getting access is not dependent on physical location. So, I do not need to be at the office and connect through the eh, Wi-Fi connection there to be able to access the VPN. I can make that connection to our [the VPN of the professional services firm] from anywhere in the world.

X: Could you tell more about the private network?

Y: The private network, so, do you mean- Because you mentioned in the beginning of our introduction that it is more about [the professional services firm]. So, are we talking about corporate VPN or also how you might use it as a private person?

X: Yes, how you use the [VPN of the professional services firm].

Y: Okay, all right, so in a corporate setting. Essentially it, it, eh, the way that it, the way that I use it is that there are certain eh, applications that are only accessible when you are within the [the professional services firm] network. So, eh, a very simple example of that is [an internal page], but also other business supporting core applications. And due to security reasons, these are not accessible just from any public Wi-Fi point. And you need to first establish eh, the VPN connection, so that the traffic is, is properly secured and encrypted, to then be able to basically use it as if you were just connecting to the office Wi-Fi. So, it allows you to feel or act as if you were connected to the office Wi-Fi and using all of the appropriate business applications irrespective of your geographic location, that is how I use it.

X: Do you use the VPN for any other purposes?

X: No, not the, not the corporate VPN.

Y: Or what other purposes are you thinking of?

X: Eh, I don't know, just getting a feel of what people use the VPN for.

Y: Yeah, so for me it is, from a business perspective, it is more to make sure that I can access whether it is [an internal page] or other type of applications, eh, [0:04:26 till 0:04:28 has been omitted], you can't get to it unless you are on the VPN, or the office network. Eh, just means that I can work.

X: Yes. And you said the connection was secured, can you tell more about how it is secured.

Y: Yeah, let me think, I don't think I can recall all the different protocols. Well essentially, VPN is like a tunneling system, right. So, you, you connect to the VPN server instead of just connecting directly to a website through an internet gateway. And that means that that tunnel needs to be set-up, it needs to be protected, and that also, and I know this is not the same for, for every eh, VPN, the type of protocols that they use and the type of security that they use in terms of encrypting the traffic within the tunnel, et cetera. So, there are several configurations, but it is ultimately about setting up the secure tunnel. Where your traffic goes through.

X: What do you mean with a tunnel?

Y: You can imagine it like an actual tunnel, I think that's- At least that's how I always learned it. So that your connection, so let's say your eh, I'm now dialing in from home, all of us are working from home, that I'm not connecting directly to a website, but I first set up a secure connection, eh, to a VPN server. That in our case is provided by [the professional services firm]. And that means that that connection basically forms a tunnel with the appropriate eh, protocols and ensuring the encryption of the traffic. Which then, to an outside viewer, or let's assume I was dialing in from you know, a [example of restaurant], and I was using their Wi-Fi, but then to make sure the traffic is not readable to everyone around us, using the VPN to shield off and basically wrap-up the traffic in a format that they can't read it.

X: Okay, is there a difference between home and the [example of a restaurant], in how you use the VPN?

Y: From a business perspective no. I connect as soon as I eh, use the Wi-Fi. Depending on where I am, you know this is a really practical situation, but I have travelled a lot for work, but if I am travelling in Europe, I probably wouldn't even use a public Wi-Fi spot, and just use my mobile data to create a hotspot. Eh, if I'm travelling somewhere where I know using my mobile data will cost [the professional services firm] 500 euros within the first five minutes of me using it, yeah, I would use it differently and would be more inclined to connect to, you know, whether that's hotel Wi-Fi or whatever it is, before connecting to the [VPN of the professional services firm].

X: Do you also use the VPN with the mobile data hotspot?

Y: Yes. That then just form the layer of first having the internet access to be able to establish the connection to the VPN server.

X: And what is a VPN server?

Y: That's basically the server that allows you- So, you know how I said that normally, normally if you, if you use internet it would be just routed through a regular eh, internet gateway. It's the same if I use internet privately at my home. And the VPN eh, server, basically sits between that and is the one that then allows us to connect to, for instance, the corporate applications.

X: Could you maybe use the whiteboard to draw how a VPN works?

Y: Anything specific? Cause that is quite a broad question.

X: Yes. Let's see that you connect from home and how does that look like.

Y: Okay. Let me see if I can find a pen. I'm hovering over the presentation, but I still don't- O, there we go. Now it's coming up. Eh, I am working from home. [start drawing 3\_1]. Okay, let's say this is me. Does this work. No, it's not the most- Can I turn, can I make the other one bigger. No.

X: You can undo an action or draw it again.

Y: Okay, let me see if I can do that. I am trying to redo- O, now it has taken everything away, great. And I want to try and type in it. So, you wanted to see connection from home, right? So, let's see, we do have a Wi-Fi connection here. Wow, this is looking like a child's drawing. And we would be connecting- Normally we would be connecting through a gateway, but eh, okay. O, god, can you still read that?

X: Yes, I can.

Y: And then from here, and I am simplifying it now, right. But eh, you would be accessing whatever resources you want, whether you want to go to [social media platform] or a different one. Now, the important thing here is I think, and I know you ask specifically about VPN in a corporate setting, but of course it is also important to mention that eh, this access, so me being able to access [social media platform], [social media platform] whatever it is, eh, is not possible anywhere you are in the world right. [start drawing 3\_2]. So, if I am trying to make this connection from say [country], then it is quite likely that there is a firewall here, that does not allow me to connect to this resource. But that is the other use case for VPN, that's not really looking at eh, the corporate perspective of it. [start drawing 3\_3]. But let's assume the corporate perspective, means that essentially, instead of going directly here, I would be, so I am just gonna mirror this from above, I would be connecting to a VPN service. Where we are setting up- Basically like a tunnel here, for our traffic to go through. So, this is again me from home, and then this would form the basis of connecting. So, it would all be routed through the VPN server. And then, in a corporate setting, here behind this VPN, so this Virtual Private Network, would sit the eh, the private corporate network. So, this would be the resources that I mentioned, like [an internal page] that I would not be able to access eh, without using a VPN. If we're talking about you know, the example that I mentioned, if you live in a country that is eh, where the internet is severely restricted, than it would allow you to actually circumvent eh, using that gateway, or rather it would allow you to connect to the VPN here and then connect to all the other resources. I hope I got that right, it has been a while since I studied VPNs.

X: No problem. How does it work if you can eh, access applications in a restricted area, like you said if you go outside of Europe and you have geographical restrictions?

Y: So, you're thinking something like [country] now?

X: Yes, for example.

Y: Yeah, so let's assume, you know, this firewall here is, is not allowing you to get to [social media platform], then VPN, and it does depend on what type of VPN you, you use, because you of course still first need to establish a connection with the VPN to then use it to be able to access the other resources through it, right. That first connection point requires the VPN server to not be blocked by the country. And I know that eh, that depending on- Cause there are a lots of companies as well that are offering subscription based VPN, some of them have been blocked in the past, but in general it means that you first pinging the VPN server, and then you know, basically that's becoming your internet gateway. So first you need to make it through here, make sure the VPN connection isn’t blocked and then once you have been able to establish this, this sits behind it, that allows you to connect to all of those resources as if you weren't even in [country].

X: How is your location determined?

Y: Based on your IP-address.

X: Sorry, can you repeat that?

Y: Based on your IP-address.

X: Okay. And could you explain to me what a server is?

Y: What a server is. So, it's part of the infrastructure that you're using to connect. It's basically eh, and it can be you know a virtual server or an actual server somewhere, it's, it's, it's well, what is the best way of describing a server. It's a connection point that facilitates the way you connect for instance with a specific web resource, a website.

X: Okay, and could you explain what a gateway is? What do you mean with a gateway?

Y: Almost like a, like a division keeper, asked to what eh, what can go where. So what are you allowed to access and it's, it's like a, you know, at school in the past when you'd cross a road and it's like telling you yes you can go here, yes you cannot go here. And normally, and that's the reason I'm mentioning it in response to restricted countries, where, you know, that it usually flows from the internet service provider in that country, so there is an element of eh, state-oversight that can be, eh, that can be applied here.

X: Okay, and on what devices do you use a VPN, the corporate VPN.

Y: We use it on our corporate laptop.

X: Only on the laptop?

Y: Yeah, I think there is actually, on the phone as well, but that is part of the eh, mobile device management. Yes, there is a VPN configuration that we can add here.

X: And what actions do you take to create a VPN connection?

Y: As a user or as eh, the IT team setting it up?

X: As a user.

Y: I first, so on the laptop, I first need to make sure eh, one second, I'm getting pinged by so many people. Okay, sorry, responded on [conferencing software]. What actions do I take. Okay, so I first establish connection to the Internet, because if you recall, we first need to be able to, to establish that connection with the server, right. So, there is an element of first setting up that connection and that requires me on my corporate laptop to have eh, internet. I either use my home Wi-Fi or if I’m travelling I'd create a mobile hotspot, which essentially acts the same. Eh, and then as soon as I’m successfully connected to eh, the internet, I open up the [the VPN of the professional services firm], click on the connect button, and then there has been some security measures built into this, eh, and what that means specifically is that it connects to a soft [access token provider] token on my phone, which provides a, I think it is an eight digit, no it's a six digit code. Which I need to enter and it is regenerated every, I think 60 seconds. So, it is constantly updated, and I need to enter that on top of entering a, that's an eight-digit personal code that only I know. And once I have successfully entered that, and it verifies that I have provided the right eh, software token, so the [access token provider], then it will allow me to connect. And it will give me an icon that says connected and then from that moment onwards I am able to use [the professional services firm] internal resources.

X: Okay. And you say you use a software token. Are there any other possibilities?

Y: Yeah, you can also use a hard token. So, we used to- We have always worked with [access token provider] as a provider at [the professional services firm], at least since I joined. In the beginning we had a physical token, which you just carried on your key chain. It had essentially the same functionality. So, it was showing the, the digits eh, I think it was also a six-digit code at the time. Which would automatically refresh at timed intervals, but that for me was a little bit more complicated, because [0:20:08 till 0:20:25 has been omitted], so I was happy when I could move my [the professional services firm] token to a soft token, [0:20:31 till 0:20:35 has been omitted].

X: I can imagine that. Is there still a possibility to have a hardware token in [the professional services firm]?

Y: That's a good question. I handed mine in when I switched to a soft token. I know at the time it was eh, optional to switch to a soft token, and I would imagine, because this was already a couple of years ago, that they would have transitioned everything to a soft token by now. Eh, but I don’t know that for sure. It is maybe possible that they, that they still use some hard tokens. No clue.

X: And why would they switch to a software token?

Y: I don’t know what prompted that decision specifically.

X: And eh, earlier you also mentioned that you do not use [the VPN of the professional services firm] when you connect to the office Wi-Fi, why is that?

Y: Because then you're actually part of the, the local area network that [the professional services firm] has set up in the office. And that does not require you to, to use the VPN server. So, if I am logging in from the office directly, it has all been configured that I connect to a specific Wi-Fi, I think it is the [the Wi-Fi of the professional services firm]. And that's essentially, so that's the Wi-Fi that you then just connect to directly. And VPN mimics as if you were connected to that Wi-Fi from the office, but from, eh, from a distance. So, it is not necessary to connect to VPN from the, from the office, since you're already part of the eh, the trusted private corporate network when you connect to the, to the dedicated Wi-Fi connection.

X: And what is the influence of a VPN connection on your computer security?

Y: On my computer security. Well, it means that eh, you know, since we do have a tunnel set up, which is, and you know I mentioned there are different protocols eh, for securing this, but it is- It already applies security measures to set up this, this path that we're taking to connect eh, to the, to the private corporate network, and it also provides eh, to encrypt the traffic that is going through the tunnel. And the level of security of course depends on the configuration of the specific VPN. The idea is that eh, you're encrypting the traffic and sending it through a secured channel. So that is the additional security measure that you take.

X: You say different protocols, could you explain a bit more about that?

Y: Yeah, I am, let me see, you might need to help me out with remembering some of them. I know there are some protocols that work, they are like an all-inclusive package essentially, that take care of both of the setting up the connection point as well as the security measures that are applied to the traffic. And then there are others that work in combination, so you'd have one protocol that allows you to create the point-to-point connection and then you would put something like IPsec on top of it to secure the traffic, and encrypt it.

X: So, you create a point-to-point connection.

Y: Hmhm.

X: What does that entail?

Y: So, you wanna connect your own connection point to the VPN server, right. This is the tunnel. So, it has a start and has an end, and it allows traffic to go back and forth. That is the point-to-point connection you're setting up.

X: And what kind of digital threats do you deal with on a normal day?

Y: What type of what threats, sorry?

X: What kind of digital threats.

Y: In a specific setting or, what do you mean when you say on a normal basis?

X: So, yes, in a normal day what kind of digital threats do you encounter?

Y: Well, that's a very, eh, there is so much, that's a very broad question. Do you mean specifically when you're not using a VPN or eh, if I'm working, if I'm looking at myself as a private individual eh, just wanna make sure that I scope the question correctly.

X: Yes, in a general sense. So, you mention there are a lot, could you give a couple of examples.

Y: Yeah, of course, and let me know, I won't be able to cover everything because it is so broad, but happy to go into more depth. Eh, so I think you know digital threats eh- We have, o god, that's such a broad question. So, anything that starts from eh, someone assuming your identity, you know whether that's the typical example of you know, a grandma being send an email to provide their banking information, or, you know in the US if you look at social security eh, numbers that have been stolen, or the BSN number in The Netherlands, so there is always a threat of someone eh, assuming your identity, pretending they are you in a digital space and using that for their benefit. Whether that benefit is, if you take the example of a social security number, that they are able to maybe apply for eh, social benefits or a loan in your name, without you having to do anything to do with it. Or if you take the more extreme example of getting access to certain payment applications or even your banking account, it means that they are able to steal money from you. So that would be eh, threat eh, that I think that eh, is quite relevant to lots of people. Depending on, on where you live, of course also, you know I mention here that certain restrictive countries might not allow you to access certain resources, but on top of that also eh, and that is a connection to the VPN connection, that you might be eh, you might be victim to someone you know, sniffing on your traffic and actually reading everything that you send through the web. Which can serve you know, multiple purposes. Eh, intentions of attackers I think are as wide as there are eh, different attack scenarios. So, whether that's with the objective of eh, getting to personal data, which we all know is a very high sought-after currency and, and can be monetized quite easily. So if I would wanna sniff the traffic to actually you know, what log in credentials you use to a specific resource, but it can also be, and this is where we are looking at different motivations, if you are severely restricted state, you might also surveil your eh, your fellow country women or men and we know the NSA scandal of mass scale surveillance, but we also certainly know that countries that are subject to a lot of restrictions eh, in terms of freedom of press, human rights et cetera, they are actually finding out information, personal information about someone, whether that reveals their political affiliation or sexual orientation, eh, can so far as costing people's lives. So, we are looking at something that goes way beyond stealing money eh, in that specific scenario. But those are just you know some very, very high level eh, examples. There are million more.

X: And from an [the professional services firm] perspective, does the threat change because of the VPN connection?

Y: Does the, does the what change, sorry?

X: Does the threat change because of the VPN connection?

Y: Eh, well some of the threats change, so when we talk about eh, sniffing traffic etcetera, you know, using the VPN as a security measure to, basically wrap up and encrypt the traffic certainly makes it way less likely, or it is associated with way more effort to get to that traffic. Eh, there are other types of threats that are not directly eh, mitigated by the eh, VPN connection, which are also you know, some of them are definitely prone to human error. So, for instance, for us always a big risk factor is eh, us accidently sharing files with the wrong recipient or making it accessible to the wrong recipient. So, that has nothing to do with the VPN connection, that’s how we behave. And also, because we have a lot of e-mail contact eh, outside of the organization, whether that's clients or vendors or other third parties, of course there's always a risk of a phishing attack or so. Which you know, whether it is human error or those types of attacks, we have different eh, security controls and measures in place, to more specifically target those.

X: Clear. And this is about digital threats, do you also deal with social threats on a normal day?

Y: Social threats?

X: Yes.

Y: Eh, is that something like looking at something like a social engineering attack or do you mean something else with a social threat? A social threat also, I mean, can also be look at socio-economic circumstances somewhere, that I would see as a much bigger threat than anything that stems from cyber or from digital devices.

X: I mean all threats that are non-digital.

Y: Then, are you looking at politics or-

X: If you imagine these kinds of non-digital threats, can you describe how those non-digital threats change because of the VPN connection?

Y: Eh, I am still trying to understand eh, the example of a non-digital social threat.

X: For example, you mentioned social engineering-

Y: Yeah.

X: That would be a social theat.

Y: Okay, but we're still looking at threats specifically looking at eh, at cyber space?

X: Not necessarily cyber space, eh, all kinds of social threats that stem from the perspective of [the professional services firm].

Y: Okay, cause I would also argue that what's going on in [country] at the moment around racism is a huge social threat, but that's not what you're looking at.

X: Not necessarily, but it can definitely be a social threat. If you see it as a social threat as well from the perspective of [the professional services firm], then yes, it is-

Y: No, it's more a broader societal thing. Yeah, but correct me if I'm not going in the direction that you're looking for, because I don't think I fully understand the question. I am using the example of social engineering, so here eh, in the example that I will talk about, VPN has very little, or very, basically a negligible role to play. So, let's talk about eh, one of our office locations, we might use the [place] office as an example, we have implemented physical security controls, we need to restrict physical access to the building, that involves [0:32:36 till 0:34:06 has been omitted], but let's assume for arguments sake, an outside person with malicious intent has managed to get into the [the professional services firm] office. [0:34:15 till 0:34:17 has been omitted], and is able to walk around freely. than they might use that to try and find a connection point into the Wi-Fi or maybe find a device that has been unlocked and not eh, secured correctly to try and get access to resources on the [the professional services firm] network. That would you know, if you were to try and do this attack from abroad, also be accessible through the VPN, but it is much more likely to be successful at an office location.

X: You mentioned shortly VPN. How does VPN, does it have a role in this?

Y: No, if we're looking at the specific example of a, of an office. And we already spoke about the fact that we do not connect to VPN, [the VPN of the professional services firm] when we're at the office. So, in that specific configuration, no.

X: Okay. And from a different location?

Y: Yeah, from a different location. So, I think, you know, hacking the VPN server is quite a momentous task, we only, this is also not a very likely scenario, but the only scenario I can think of is let's assume I'm with my laptop eh, in [country], I was working from it somewhere in a hotel lobby, I am connected to the [the VPN of the professional services firm] and then the, the easiest point of attack would be to distract me, so that I leave my laptop unattended and that I haven't locked it. So, then someone would be able to exploit the fact that I am already connected to the VPN, so I have virtual access to the private corporate network. And use the resources, at least the resources that are accessible to me in that scenario. Because I am not an admin, I don't have access to all files and resources at [the professional services firm] either, to try and obtain that data.

X: What do you mean with you do not have access to all eh, files because you're not an admin?

Y: Yes, so as any organization, we have identity and access management controls implemented. What that means is that in line with your, in our case it is a role-based access system, eh, in line with your business role, which needs to be validated upon hiring and also is in line with your eh, functional role. You only get access to the eh, the minimum of resources that you require. And you do not by default get access to every resource the way that a system administrator would, absolutely not.

X: How would that look like in the drawing you made?

Y: Eh, don't know if we can add it here. Can I just add something new? Or do you need me to add it to this one?

X: O, a new slide you mean?

Y: Yeah.

X: Yes, that's possible.

Y: Let's see. [start drawing 3\_4]. So, the way that it works is, let's assume something like this. Eh, that person is a little bit ill-shaped, but that's okay. We all look different. Let’s assume this is me, so this is [role], this is an admin, and we are all connecting to the different resources, and- Slowly getting the hang of the drawing. Okay. I spoke to early, should connect here. All right. So eh, let's assume, you know, we wanna connect to the different resources, whether that's [an internal page] or just a general office eh, core business applications that we’re are using as [the professional services firm]. Eh, but we are different people connecting to this. And if we are on a, you know, at [the professional services firm] office, this would allow us to do that directly from the office Wi-Fi that has been configured. If not, it will go through the VPN. But it's the same process. So based on your role, you will have different access privileges. So, for instance, we discussed I’m a [role], which means I need certain access to applications. So, for instance, I will just give you an example of that, I need edit or write access to eh, I can't think of the perfect example, but I'll just use [an internal page] for now. This is not the best example, but just for argument sake, right. Eh, then we have [role], who needs no access to [an internal page], and then we might have, and bear in mind, this is not how [an internal page] works, but I just wanna illustrate how it works. Then we might have a third person from a business perspective, that could be eh, someone from I don’t know, maybe another function, another team or so, that only requires- [start drawing 3\_5]. The idea behind this is that depending on our access profiles, so these here, are our roles, no that's not working yet, for instance, if [role] were to try based on their business role and their access profile to connect to whether that's through the office Wi-Fi or a VPN, to let's assume it is this one, that we're trying to connect to. [start drawing 3\_6]. I'm sorry Veroniek, there are so many people pinging me and trying to call me. Eh, let's assume this is the resource we wanna get to. So, this is [an internal page] in this, this hypothetical example. Depending on the business role that you have, this person would only require read-only access, so they would not see the same that I see as the one that needs to be able to edit and write, [0:42:20 till 0:42:23 has been omitted]. And since that's a business process [role] is not involved with, [role] doesn't need any access at all and thereby we are implementing the principle of you know, least privilege, and ensuring that only the people who really need have access to it.

X: And then eh, all lines go to the circle in the middle-

Y: You mean the yellow one or this one?

X: Yes, this one.

Y: This one?

X: Yes, this one.

Y: Yeah, so this one would be eh, you know, whether it's the connection which has been facilitated through the Wi-Fi that has been configured at the office, or, you know, the VPN is first giving us access to that virtual private eh, the virtual private corporate network.

X: And then going back to the attacks we mentioned, who or what could be an attacker behind it?

Y: Eh, are you thinking of a specific threat?

X: For example, social engineering you mentioned.

Y: Hmhm. Well, I think the threat remains the same, that it's a malicious actor trying to get access, eh, so that's not a variable that is, is changed by this. However, of course as an attacker you're trying to maximize the access that you will have, to maximize the impact you will have. So, if I manage to get access to [role] and let's assume my ultimate target is to see [an internal page], that would be no good. Because from [role] account, there is actually no associated business role and rights to access that. So of course, from that perspective, you'd try and go for a business role that has access. So, [0:44:37 till 0:44:37 has been omitted], to be able to get to it, and ultimately the goal of any attacker is to try and elevate their access and their privileges to the point that they can take over a system. Eh, so that they can freely navigate and find whatever they are after.

X: What kind of malicious actors are we talking about?

Y: We're talking about a lot of different of them. So you can think of eh, in a corporate setting, eh, you know, maybe it's a disgruntled ex-employee, maybe it's corporate espionage, eh, but many, many more, I mean there are as many motivations and actors that you can think of, but these are probably eh, the most relevant in this context.

X: Could you give examples of their motivation?

Y: Well, disgruntled ex-employee, I think that's eh, the clue is in the title, so if they feel they haven’t been treated fairly, they might try and get access to be able to expose certain files that they feel would be damaging to the company, or that they would wanna use in building up a law case against them for instance. Corporate espionage, I think again, the clue is kind of in the title, so trying to access any type of information that would give you eh, a competitive advantage going up against that company. That's probably less so relevant for us, but if you're imagining you working for a big pharmaceutical company, that has eh, you know, eh, proprietary recipes, you know, that have not yet, that are still patented, so you haven't released the formula et cetera, than getting your hands on that eh, would give you a huge advantage in being able to tackle that company's, maybe even monopoly on producing that specific drug.

X: What would be an attacker’s capability?

Y: Capability?

X: Yes.

Y: Their capability, that's looking at their own eh, I think capability mainly looks at your own expertise. And your own- So, your starting point. So are you skilled at hacking, do you have any social connections to the company that might allow you to sneak your way in, eh, do you have access to people that will pay you to do this job, or maybe on the flip side, are you the one who has lots of money and you can hire a big group to do this for you. All of this are examples eh, but not exhaustive in terms of capability.

X: Okay. Does the kind of attacker change because of the VPN connection?

Y: The kind of attacker?

X: Yes. So, the sort of attacker.

Y: Eh, well, I, I, yes, do you mean change in, in what sense specifically? Cause of course our attack scenarios don't really have a VPN connection at the center of them. So eh, disgruntled employee, so what might happen, you know, what, this is, this is not something that's really relevant in this scenario, but let's assume hypothetically the company has very poor of boarding of employees, so the leaver part of the join and leave process which is a core aspect of your identity and access management doesn’t function properly and they do not remove your access on time, so they don’t disable your account, so the account that would be associated with your business role and the profile that you'd get with it and on top of that, not only do they don’t do that, but they also don't ask you to eh, return the token, so we're using the example that we, that we used earlier that you require those levels of access controls to it. Then in theory you'd still be able to access company resources, even after having been terminated. So, you're still able to get to the VPN connections, because your user credentials as whatever else you might need, so in this instance a token hasn’t been taken away from you. And then you're able to access company confidential information, even after having been terminated.

X: Very clear example. And if you look at an attacker’s motivation or skill level, would that change because of the VPN connection? If you use a VPN connection?

Y: Eh, that's quite broad to answer definitively, so I’ll try and make it example based. So, in this example that I just mentioned I don’t think capabilities have a lot to do with it. Its more that a person doesn’t need to understand how a VPN works from a technical point of view to be able to take advantage of the fact that their access hasn’t been disabled on time. They just need to you know figure out that they can still get access. Eh, and then use that to get to whatever information they want to. If we using an attack scenario which has not got a disgruntled ex-employee with insufficiently terminated access rights, so someone who's starting, you know, completely outside of the company, then yes, and let’s assume you're not trying to orchestrate a social engineering attack, which means getting physical access to the building. But you actually wanna try and hack the VPN connection, yes of course. Because there are additional security levels, thus, to be able to actually break the VPN, that eh, requires tremendous abilities and capabilities. If you look at the example like the one I mentioned earlier, that I am working from the hotel lobby in [country] and someone tries to distract me to make sure that I don’t lock my laptop and its connected to the VPN at that point, that doesn’t require a lot of capabilities. But it does mean that you’d only see whatever I have access to and then being able to elevate those rights and jump around and ultimately try and get admin access, yes, that’s again of course requiring a lot of capabilities.

X: What could be the impact of an attack for [the professional services firm]?

Y: So, let's go smallest to biggest. So if we assume that in one of those two examples, so disgruntled ex-employee or someone manages to get my laptop unlocked while I'm already connected to VPN, they would be able to access any information that I am allowed to see, based on my business role. So they would be able to see all my files with client confidential information, they would also be able to see confidential commercial data that I have access to, which eh, they would be able to, you know, take copies of or extract from the system, and then be able to use to whatever advantage eh, they might want. Depending of course on the individual eh, motivation. If you take worse case and someone uses the connection into the system, whether that’s on premise or through a virtual VPN connection to try and elevate and escalate their privileges, then you could be looking at them getting access to even more data. But ultimately, it's about, at least from the type of scenarios that we're dealing with, its mainly about getting access to confidential data and being able to use that.

X: What could be a consequence if they get access to that confidential data?

Y: Well, it’s a breach right, it’s a data breach at that moment. And it needs to be investigated and followed appropriately to determine the impact and could be subject to, you know, having to notify the data protection authorities, could even possibly lead to fines if we're found to be negligent or depending on the impact and we also need to look at notification chains with anyone that's affected, which of course if you imagine that that’s a client, will not necessarily help our relationship with them and might even bring with it legal consequences in terms of lawsuits.

X: Okay. And if we look at the VPN connection itself, how secure is the VPN connection?

Y: Yes, so this is where I mentioned earlier that eh, just because it says VPN, there are still varying levels of security within that connection, because it ultimately depends on how you set it up and which protocols you use. And I know that some of the initial protocols that were used have been, you know, the encryption behind them has been broken, eh, so yes, it offers you an extra level of security in terms of security and keeping data confidential and setting up the, the connection to the private network so that you're not spied on essentially as you're, as you're connecting. But ultimately if you want to have a definitive conclusion on how secure it is, you need to look at the specific configuration of the VPN. You can't make a default blanked statement.

X: And do your actions change because of these insecurities?

Y: My actions change based on the insecurity?

X: Yes. So, do you handle differently, because you know there might be vulnerabilities in the VPN connection?

Y: No, they don't, because ultimately, I need to work, I need to get access to it. It's still way more secure than if I was able to all company resources from [example of restaurant] Wi-Fi. Eh, the reason that I emphasize that it depends on it is that in, as with any you know, security mechanism that you deployed, always depends on the specific configuration. But eh, having said that, having a VPN to access the corporate private network is from a security point of view way more preferable than not having one. But that doesn’t mean, and that is I think in general with security, that you're never gonna have a 100%.

X: Okay, I think that is a nice notion to end this on. Do you have anything about VPN that was not said right now?

Y: Eh, no nothing from my side. I know it has been quite free format in terms of covering topics, so I don’t know if we've covered everything that you wanted to get into.

X: Yes, we did. All questions I have are answered.

Y: Cool.

X: So yes, if you can think of anything that we did not speak about and that you think is important to mention-

Y: Let me see, well the only thing that, but this is not, this is really not from a corporate point of view, but more a, eh, societal view, because I do think that, you know, how I said in that previous drawing I said well you first need to establish a connection to the VPN server.

X: Yes.

Y: Which I know in certain countries also, if it's a recognized VPN service, they might actually disable that eh, that connection. So, I know that, I think the NSA did that as well, that they actually were scanning for people using a VPN or you know, using their search terms to connect to a VPN and then put them on a list of people requiring, eh, more surveillance, because they felt that was by default suspicious, that someone would try and, and keep their web traffic and those connections private. So, I think that's more a political point of view. And from an individual perspective of course I feel like we're all entitled to not be surveilled by a state, but then there is also the flip side of it, if you look at it more eh, from a law enforcement point of view, then of course eh, privatizing, or not privatizing, but keeping information private and allowing people the freedom that comes with it, of you know, either using a VPN service or even setting up their own VPN does mean that, of course it can offer those people with malicious intent and criminals also a way to hide from law enforcement or make it significantly more difficult eh, to get to them. So, I think that's just one, it, it's not related to VPN in corporate use, but more from broader societal perspective. It's something to be aware of that what we're gaining from it is also avoiding eh, more privacy and freedom to those with definitely not the right intent.

X: From an [the professional services firm] perspective, is the NSA for example, taken into account searching for a VPN connection or making a VPN connection eh, and placing the [the professional services firm] employees on extra surveillance, would that pose a risk?

Y: Yeah, I don’t know how likely that is, because of course you also see what kind of VPN service you connect to, and if it of a very reputable firm, that's definitely something different than you know a guy from Minnesota that has suspicious spikes in web traffic anyway, using a eh, a custom built VPN. So I am, yes of course you could argue that this is also important in a corporate setting eh, but I think this is more, and that's why I say for me it is more a societal point of view, this is probably something that proportionally will affect individuals or you know groups of political activist more than it would a corporate. That's just a personal gut feeling, I don’t have any stats to back that up.

X: Okay. Thank you very much-

Y: You're welcome.

X: I think that was everything from my side.

Y: Cool, hope it's helpful.