00:00:01  
*Speaker 1:* Can you introduce yourself a little bit? Sure.

00:00:03  
*Speaker 2:* Um, my name is Alex Simonsen. I'm information security consultant here. Uh, I've been working with, uh, cybersecurity for the last ten years or so. Starting as an external consultant in a private consulting company. Then I work in, uh, uh, one of these systems, the Ministry of Education. I worked there for, like, four years. I started here in, uh, Mitchell in December. So it's like, what, 4 or 5 months ago? So. But the basics working with cybersecurity is, is the same in the Ministry of Education. There was more on the GDPR side, protecting, uh, kids and young adults. Uh, data here. It's more on the technical side. Uh, working with that angle said change a bit.

00:00:58  
*Speaker 1:* So how interconnected are Denver's metro control system with other critical digital infrastructures, and what potential cascading failure scenarios concern you most?

00:01:11  
*Speaker 2:* Well, okay. Once again please. How are we connected to what?

00:01:16  
*Speaker 1:* How are you interconnected in the overall critical digital infrastructure.

00:01:23  
*Speaker 2:* Mhm. And I will ask you in another way because we are what you call critical infrastructure because we're running trains. Uh, but then again, uh, it's a little, a little bit technical. We are the, uh, constructing part of Metro. We're building the stations, the tracks and stuff like that. Our sister company, Metro Service, is the one running the trains. They're part of critical infrastructure. We're actually not really, but our owners. This is 50%. The state, 25%. Copenhagen Municipality 25%. Flexibility that part of critical infrastructure. So we have decided we better be there to regarding to this to, um, regulation coming up here this summer. So we decided to do that. If that's the answer your question, I'm not quite sure.

00:02:22  
*Speaker 1:* How would you reflect on the hybrid warfare in relation to my thesis? I described the health care sector, but how would you reflect on the transportation sector?

00:02:33  
*Speaker 2:* Well, we are very, very aware of that because, uh, the level of threats and the level of uh, attacks has increased like 300% after the Ukraine war. Um, that's a direct quote from the global. Uh, si, si. So from um, mask uh, that there and that actually six month ago, there might have been crazy. Even more so. Definitely. We are attacked massively. Anybody else? Uh, so it's a very high, uh, on our agenda always to, uh, to sort of, uh, push back on that, uh, because everybody is attack right now. This is not a matter of, uh, if you're going to be attacked, it's, uh, it's about when basically.

00:03:32  
*Speaker 1:* So in relation to the adversaries, who are your most concerned countries that are possessing the most danger right now?

00:03:42  
*Speaker 2:* Russia, no doubt, Russia and China.

00:03:46  
*Speaker 1:* Could you speculate why? Why you think so?

00:03:49  
*Speaker 2:* But I'm, uh, I'm attending a very large. Uh, of course, I got a lot of, uh, emails, uh, from different, uh, cybersecurity groups, uh, always discussing and informing each other. Uh, I'm attending a lot of cybersecurity. Uh, uh, what do you call, like, courses and what's missing in English? I don't know. Uh, large groups, uh, discussions, uh, all the time. That's a massive, uh, general, uh, the point. All the or at least a large part of the arrows points towards Russia. No doubt.

00:04:34  
*Speaker 1:* How would you describe the awareness level of your colleagues that are not related to the IT department, for example, about the cybercrime.

00:04:42  
*Speaker 2:* In this company? Yeah. No, actually it is because, uh, we just entered this company like four months ago. And was actually surprised that the awareness level was quite low. Uh, and my angle on the awareness is like the, uh, employees of the company is the largest. Uh, uh, what do you call it? Uh uh. Hang on. Uh uh, the strength as well as the weakness and this difference between those two. That's awareness. Right? Actually, I could give it to you. This one just. It's like a two month. One month ago, I introduced this code of conduct to all the employees. It's a information security policy written, uh, at the employee level. What are you, as an employee is going to do? Have to be aware of. And it's, uh, literally written in a little simple language. Very straightforward. What are you going to do? And not, uh, to increase the awareness level? Uh, and we're just, uh, we're running a lot of, uh, you can see this one. It's it's not very academic, but basically this is why is awareness, uh, uh, important? You see all the technical part, the one side, and then we got the human error and the other part that goes for everybody. It's not very academic. No, but that's the truth. That's what's going on. Uh, I think approximately 40% of the employees, when leaving the computer, they don't lock the screen. This is about leaving your home with the your front door wide open. Uh, so we're going to introduce a campaign next week. Uh, we're going to walk through all the offices in the middle of the lunch break, uh, testing who's capitalism and who's not. So yeah, but it is very, very low. The level of awareness is low. Unfortunately it is. So that's why we're working at that one.

00:06:53  
*Speaker 1:* Would you say that it is based on the cultural thing that the Denmark is a trust based society? Yeah.

00:07:01  
*Speaker 2:* Which the trust based part is actually positive as being one of the most digitalised countries in or being a very digitalized country is good. When you combine those two against. Uh, cybercrime is very bad. So it is and you write about it as well. So we, uh, um, we are vulnerable as a country. Um, so most of the people. Well, this is great. We are very digitalized. We are very, um, sort of, uh, uh, polite, trust each other. We were very trustworthy. Period. They do not connect that to cybersecurity. And that's the issue. Definitely.

00:07:45  
*Speaker 1:* How would you reflect about the legacy systems in your company. For example, do you use any old outdated systems to run some processes?

00:07:55  
*Speaker 2:* Uh, no, actually not because we're quite a young company. We're only 23 years old. Uh, we just started 20 just 23 years ago. I know your age. It's, uh, like 2000 years. I know we were quite young. So the system is actually quite young. So, no, we don't have any legacy system. As far as I know. I mean, I don't believe for a month, um.

00:08:21  
*Speaker 1:* What? Physical digital security intersections present the most complex challenges in metro security management.

00:08:32  
*Speaker 2:* Um, I need to talk about the metro gate. The one the construction company. The part where I'm placed in. Because the other one. Metro service. Who's running the train? I'm not working with. so I don't need to know that. Um, please repeat your question.

00:08:51  
*Speaker 1:* So what are the basically weaknesses in the physical digital infrastructure of the metro?

00:09:00  
*Speaker 2:* Um. I think the maturity level is low. We have, uh, what is called Microsoft 365 defender. It's very advanced. Uh, systems protect us. We paid a lot of money, but nobody has ever installed it. And so it works. And that, uh, when I found out, I was like, okay, well, we need to call some guys into to to set that up, and we're running a do you know what system at 18 is about? Okay. If you if you think that like a pyramid at the top, you got the policies. This is about what are we going to do? This is about the. Why? Cyber security. The next level. Uh, ISO 2021. You know that. But that's a, uh, that's a, uh, security standard. This is about who's going to do it. And this is an 18 complex. This is about how you're going to do it at a very concrete detail, technical level. Nobody in this company knows anything about that. So we're calling in some external experts to help us. Sort of. Okay. What is your level right now? Uh. Step one. Step two. Okay. How are we going to go from here to increase the level, which will take 1 or 2 years or something. And part of that is we got this Microsoft 365 defender system, but nobody knew how to use it. And that will, uh, help us, uh, prevent some of the cyber attacks. So it's a journey. We're moving on. And the only thing will be there in, like, 2 or 3 years or something. And that's about, uh. That's about investments. Uh, an investment. That's a cost benefit thing. What part of that money. And the other part is resources. Uh, we are lacking of competent resources in the company. Everybody is. Because there's a lack of guys like you and me, by the way. So, uh. So it's a matter. It's a cost benefit going on all the time. I can show you a figure. We could. I can show you that later on. Uh, the cost benefit that's always running about risk, uh, in the company.

00:11:18  
*Speaker 1:* How would you describe the political influence on the Metro Metro's security and the whole transportation sector? Security?

00:11:29  
*Speaker 2:* But that's what I talked about earlier. The next two coming up. Uh, and the interesting part of that is the the responsibility goes all the way to the board, and when the board has something on the wrist, it will make you turn the other way around. Okay. How am I going to, uh, to, um, I'm going to to. Uh, comply with this, uh, new set of rules. Uh, and that's going to be a board meeting in 2 or 3 weeks. We just had a new, uh, chairman of the board, uh, Tom Atlas, if you know who he is. Okay. Yeah. Okay. But anyway, uh, he's going to new, uh. And he's definitely very much aware. Okay, there's a new set of rules coming up. Uh, what does that mean to our company? What does that mean to the board members? Uh, so definitely there's awareness of that.

00:12:29  
*Speaker 1:* In my thesis, I described that some public companies, they like the centralized, centralized system of command. Um. Would you? Based on my thesis. Would you improve something in your company structure?

00:12:46  
*Speaker 2:* The company structure? Meaning what?

00:12:48  
*Speaker 1:* Meaning like issue happens and you know to whom to go with this issue?

00:12:53  
*Speaker 2:* Yeah. Uh, very good question. We are working on that right now. Uh, I have, um, uh, we have this, uh, plan that's called, uh. Uh.

00:13:11  
*Speaker 1:* What's it called in English language?

00:13:13  
*Speaker 2:* Yeah. Okay. Uh, what? Basically, that's the plan. Okay. If we if there is an incident, who's going to do what and when? Right. That plan, uh, didn't wasn't very good. I just rewritten it. We're going to do a, uh, table test of that. Uh, meaning we're going to run a scenario. Okay. Now we have this incident, then that's going to happen a lot of things. And based on that we will rewrite the the policy. Uh, we just, uh, have just had a meeting this morning about creating what we call a war room. Meaning if the incident, we had some standalone computers, uh, some backup, uh, batteries and stuff like that. Um, and some update is specific software on those computers. Standalone. So we're just about to establish that that happened. That's not been in the company before I asked for. Uh, it's going to happen. So that will be established within two weeks or something. So that's what I'm going to talk about. The maturity level of this company is quite low. I'm pushing to, uh, increase the maturity level.

00:14:28  
*Speaker 1:* How would you, I would say reflect that my thesis brings up the the current problems of the digitalization. If you were, for example, the ITC chef. Of the whole department, how would it affect you and your thoughts about your company?

00:14:49  
*Speaker 2:* The increase? Well, we are at a very high digital level. So the question is if we increase that level or I'm not sure. Okay. If you increase it even more.

00:15:03  
*Speaker 1:* Yeah. So basically what will be the trade off between the digitalization and for example, passenger convenience. As far as I know that metros they don't have a driver. So basically they are fully operated by the systems. Yeah. How would you I would say secure the passenger security, since there is a huge development in the AI and quantum computing since, for example, like if hacker is infiltrating your systems, the passenger's life can be on the line.

00:15:36  
*Speaker 2:* Sure. But. Yeah. Yeah, yeah. That's always a trade off. Because on the other hand, it could be completely manual. A driver running the trains. Uh, but then again, the the system, uh, telling the trains when to stop, when to go. Uh, it's it's automatically now, uh, the trade off. It's somebody. Should a person or persons should push a button. Red green light and stuff like that. They can make false as well. And that system has to, uh, send signals out on the tracks. That could be hacked as well. So it's a trade off of how, um, uh, the efficiency, uh, and the cost, because all the drivers, the one pushing the buttons cost money. On the other hand, uh, the technology, of course, costs some money, but it's much faster, and it's much more efficient. And especially when you're running metro trains, which is running every second minute. Uh, that kind of a train. It's very difficult to have that manual control because it's simply not fast enough. Uh, so it's sort of the trade off if you're going to run it manually, let's call it that. Uh, the number of trains has to be reduced, and then the efficiency of the whole metro system is going to be reduced. Right now we're running some of the, the tracks, uh, are running, uh, over 100% the more than 100% filled. So we have to let's say we should go do a little more manual. Uh, it will go up like 250% with with the result that crashed. That wouldn't be good enough if you understand my. So it's simply not possible for us. Because if we should do that, then we need double tracks all over the place, which we call Billions of occurrences. That's that's not possible to do that. That's a practical side of it. The other one, that of course, uh, uh, bring us in a vulnerability because we are running very high tech system, which again, is quantum computing, which will come up in like five, ten years or whatever, uh, will make us vulnerable. Yes it will. We have very aware of that. There's a lot of security built in in our systems. Uh, also also the very low practical part, if there's, uh, there's just been a major electrical electricity, uh, cut off in southern Europe. What happens if that happens in Denmark? What about the if the a lot of the metro system runs underground? What if the systems or the tracks are getting flooded by water? What are we going to do about that? There's a lot of security building in our systems. And by the way, you can't run the, uh, metro manually. It's possible because in the front there's a panel, you can't see it, but there's a panel. You can run it manually if you know how to do that, that you can't do that. But that's the secret.

00:18:52  
*Speaker 1:* So basically, once when I was, uh, using the Metro, I saw that some of the panels on the top, they fell off and there were some physical, uh, the courts interconnected. How would you say that it would affect the threat level.

00:19:11  
*Speaker 2:* If if what.

00:19:13  
*Speaker 1:* If, for example, if someone decides to open the panel and, like, do something there?

00:19:19  
*Speaker 2:* Well, that's a possibility. Sure. Uh, yeah. But I don't know, you could call that a cyber risk, but it's it's a more. I don't know, damaging the train, so I don't know. I don't think it's a related, uh, risk. What are you talking about there? Yeah. Of course you can cut cables. You can put things on the tracks. Yeah. Okay. Then we have problems, right? Um. But all the trains are programmed. If something happens, they should always, uh, continue to the nearest platform to get the passengers off. Of course, if the system or the electricity is blocked, more like, I think 15 minutes. Uh, then all doors open and people have to walk through, uh, the, the, uh, the channels to get to the station. That's a major problem because before starting up the trains again, there's metro workers who's had to go magnetic Go walk all the all the systems to check this or to check there's no passengers. Uh, so that check 1 or 2 hours before we can start again. Um.

00:20:39  
*Speaker 1:* Uh, have you read about the recent incident this week that some of the European countries were left out without electricity?

00:20:46  
*Speaker 2:* Yeah. Southern Europe? Yes.

00:20:48  
*Speaker 1:* How would you reflect on it in comparison to Denmark? What would be the outcome of the same situation in Denmark?

00:20:55  
*Speaker 2:* Completely chaos because the digitization level. All our phones are dead. Um, uh, my car is, uh, Tesla. I can't even open the door without my, uh, without, uh, uh, electricity on my phone. Uh, then at some level, there's I can't drive any further because my gasoline is, uh, electricity. Uh, and actually, I don't have a credit card on me. Any longer? Only use my phone. But I'm not able to pay for anything. Uh, there's been completely chaos in Denmark. Denmark at the cessation level is very, very vulnerable regarding to cut off electricity.

00:21:40  
*Speaker 1:* How would you say that were dependent on the collaboration with external countries, for example us? You mentioned that you use a Microsoft based solutions to monitor the security risks. Yeah. How would you I would say, reflect on the development of the US politics towards Denmark and how it affected the whole security understanding.

00:22:04  
*Speaker 2:* It has, definitely, because as you write, it's 90% something of data worldwide is placed on a certain place in the US. That's a problem. Um, there's a growing, uh, in the discussion groups, uh, I mean, regarding cyber security. There's, uh. There's a growing, uh, concern about what's going on in us. Definitely. Uh, we're talking about Amazon with all the, uh, data. We're talking about Microsoft. Uh, Microsoft Office will be, if that is, I think like 90% plus of all offices, um, both private and public in terms of using Microsoft Office, if that system is blocked in some way from from us, uh, that's going to be a major problem because, I mean, all the emails going on, it's a Gmail that's on us as well, Microsoft Office, that's American as well. So that's a growing level of concern, uh, about how to move on from here because, uh, uh, the US based software company, is not as reliable any longer as it has been, so I think there will be, at a European level, growing interest of placing data centres controlled in Europe, controlled by European countries, definitely. Uh, and that will increase because this, uh, crazy clown in the white House definitely pushed the awareness level of how dependent we are on American companies. So I think from now, going forward, there will be, uh, more focus on placing both software systems as well as software centers in Europe. But that's that's not going to happen overnight because it's massive investment has to be in, in, uh, software development for one thing. And the other thing, all these software or the data centers that has to be built because the cloud is very physically placed in data centers, which cost a fortune, but I think there will be a turn from now going on for like four or 5 or 6 years, and then Europe will probably change to that place. The data in Europe controlled by European companies. Definitely. That's my definitely there's been this has been a wake up call having Trump placed in the white House with all his crazy ideas. Uh, yeah. So that's definitely been a wake up call because everybody that has been aware of that for a while, um, uh, that definitely is a wake up call.

00:25:04  
*Speaker 1:* How would you say that my thesis affected your thinking? Did it support some of your hypothesis that you already knew which new knowledge it didn't bring to you?

00:25:18  
*Speaker 2:* But I think it's interesting, your angle on Ukraine. How the how? Because Ukraine definitely is a country being attacked at the most from Russia. Um, and the thinking about okay, the, the lessons learned in Ukraine. How can we learn from that? Uh, going on to the rest of Europe. That's quite an interesting angle. I never thought about that, but that is very interesting. That's a very. If you put it on through to the more military use. Denmark is now sending a military personnel to Ukraine to learn about, uh, what you call these, uh, the drone technology. Ukraine is very, very good at probably the best in the world. Is that quite interesting? All the lessons learned in Ukraine. Uh, Europe is dying. Okay. These guys really have built up a capability at an extremely high level. The rest of the Europe, the rest of the world can learn. So that's quite interesting. I never thought about that. So when I read this and say, okay, just compared with the Danish soldiers moving on to Ukraine to learn about the drone technology, it's a bit in the same, same pattern. So that's quite interesting. Angle.

00:26:32  
*Speaker 1:* Which I would say recommendations you can give on supplementing the theories that they made, for example, like on the political tensions between countries and how vulnerable the cyber space is.

00:26:54  
*Speaker 2:* Interesting, because I think the main thing for Europe especially, is through what we just talked about moving the software capability and the, uh, data centers into Europe to get on a larger scale, more stable system. Definitely. uh. But then again, I think Denmark, as digitalized as it is, is, per definition, honorable? Yes it is. And that's a. Yeah, I can show you a figure later on. It's, it's it's this, uh, we talked a bit about it when the trend is this cost benefit trade, you always do if you if you're going to run the metro company extremely efficient, it has to be at a technical, very high level. Yeah. With machine vulnerable. On the other hand if you do it low tech, you are running it less uh, at a very, uh it's not that efficient any longer. So it's a trade off always doing that. So, uh, when we Denmark is one of those. Well, even though we don't have. Yeah, we have a little gas and oil, uh, but we don't have any natural resources. Then again, it's is one of the most wealthy countries in the world. That's because of very, very high efficiency, due to the very high level of, uh, digitalization. Uh, just very, very low practical. I have my daughter. She's just, uh, a little younger, younger than you. And she's right now staying in France. She's she's amazed at the very low level of digitalization. How can they run the systems? Completely impossible. Okay. This is how Denmark was like 50 years ago. And that's just whoa. It's so. And then I have to fill this out in the hand, go to somebody who's going to stamp it, then to somebody. It's very low in Denmark that will be five clicks on mobile phone and then it's done. Uh, so that's one of the reasons why the Denmark is that, uh, wealthy because of the very high level of technology used.

00:29:04  
*Speaker 1:* Would you say that they might add app introduction to the current systems? Does it bring I would say comfort for you to use it. Or does it bring you also like some sort of, uh, concerns?

00:29:20  
*Speaker 2:* But then again, that's a trade off about efficiency running towards uh, uh, as some security. And that that is a trade off going on all the time.

00:29:34  
*Speaker 1:* Did did it affect you that, for example, like I mentioned in my thesis, that some people can reverse engineer the app, for example, like some of the students from my university, they did the reverse engineering of the media. Yeah. And they found some, uh, I would say, backdoors to enter it and enumerate the users. Yeah. And it can compromise in private information. Did it make you feel, I would say, uncomfortable a little bit about the digitalization or, you.

00:30:05  
*Speaker 2:* Know, not really because I know it already because there's these specters concept would be naive to, uh. Because I do know they exist. Uh, that's the interesting part of working with security, because the technology is evolving all the time. The the laws are changing all the time. And then the, the hackers is changing all the time. That's why even though I'm turning gray, I'm almost 60. The, the this, uh, uh, cyber security thing is, uh, always changing, which makes it makes it interesting all the time. So I hope you and your skills, your guys working on working with cyber security becomes extremely interesting because that that, uh, development never ends. It goes on forever. And our job is working with cybersecurity in a company that is trying to stay just a little ahead of the. The hackers hope so. It doesn't always succeed. But that's that's our job to do that.

00:31:03  
*Speaker 1:* Which recommendations would you have for the upcoming generation of the cybersecurity specialist based on what you read. Based on what you have experienced yourself.

00:31:18  
*Speaker 2:* First of all, we are in a very, very comfortable situation because there's less to, uh, there's a massive lack of you guys. You have a job security and a salary level at a very high. So congratulations. Oh, yeah. So that's, uh. Are we always discussing that? We, uh. That's the way too few of specialists working, uh, with, uh, skills in cybersecurity, so don't worry. You have a brilliant career in front of you. I mean, it, I mean, don't worry at all. Uh, and then just go ahead. Uh, I think, um, on the practical level, it could be, uh, both work just as an external consultant, uh, Educating both private and public companies. That's a career path to go. You can work in public companies like ministries or in private companies like this one. But my recommendation basically do all of that because you get different kinds of, uh, angles and different kinds of skills. Uh, so basically try it all. You can definitely change. I started working with I'm original educated as, uh, economist. Uh, been working with, uh, uh, financial planning for like, 25, 28 years and changed career path when I turned 50. Uh, I'm 60 now, and it's been incredible last ten years. Uh, so there's definitely you just jump into it a try. Different career, career path. Um, both, uh, public and private companies.

00:33:00  
*Speaker 1:* Yeah. I don't have any more questions.

00:33:02  
*Speaker 2:* Okay. Um, let me just show this one. I can mail it to you.