00:00:00  
*Speaker 1:* My phone ran up the battery, so I hope it will work now.

00:00:06  
*Speaker 2:* Yeah. If, uh, if it's uncomfortable, we can just reschedule the meeting.

00:00:13  
*Speaker 1:* How much? How many questions do you have left?

00:00:15  
*Speaker 2:* I have only two questions left. Two. Three questions.

00:00:19  
*Speaker 1:* Okay, let's let's go with that.

00:00:22  
*Speaker 2:* So how can technologies like AI and blockchain be lever to improve cybersecurity in Denmark?

00:00:34  
*Speaker 1:* On critical infrastructure. Um, yeah. Should we finish with the ones on the critical infrastructure first?

00:00:40  
*Speaker 2:* Oh, yeah. Sure.

00:00:42  
*Speaker 1:* Because before I left, uh, you ask, uh, what your critical infrastructure do. Yeah. I think oh, yeah. I think critical infrastructure is different from what many other companies need to do because they are the target of not only cybercriminals who are maybe more optimistic, but they are also the target for, uh, more advanced threats, which can be expensive to do. And there is a willingness to, to invest in making these more expensive attacks or more attacks to become more resources, more skilled, small time. So I think you really need to work on both the risk assessment, of course, to find out what is most critical in your processes. You need to think together cyber risk and other kind of risk, for example the physical risk. When doing the risk assessment, you need to be much more critical in terms of assessing your sub suppliers and your supply chain. Um, so the whole risk identification is much more, uh, much bigger and also more even more important than for other companies. And then I think you need to work through the whole chain of doing the right protection, the right detection. and and also having the ability to respond and recover. And you need to be really a good in every aspect of the chain. So and you and your need to understand that is not just a one time exercise. It's actually something you need to do and cannot. See.

00:02:23  
*Speaker 2:* So continue with the question about the digitalization in Denmark. So since we have a lot of digitalized services such as metro trains, what danger can it poses for the society if, for example, the transportation chain will go under the cyberattack?

00:02:44  
*Speaker 1:* I think it's. One sector, but it's taking multiple sectors at the same time. Um, Because this is where we can create more damage and more uncertainty. And this is maybe also why it's more difficult to predict when you can predict what happens if the transport sector doesn't work. It's pretty. I wouldn't say it's obvious, but you can imagine that you have no trains, no cars, no people cannot move. But what happens when you are hitting, for example, um, the telecommunications sector. So people also cannot commute. We cannot communicate with each other. You may be afraid of what's happening to people, to your loved ones. Um, and you are unable to get clarification about the situation. This is where. So these attacks that hit multiple sectors at the same time. I think it's a concern. And also attacks where it's not only cyber but cyber combined with other types of attacks.

00:03:51  
*Speaker 2:* Would you would you consider the cyber crime the attack Tech for, for example, the health care institution or would it be the cyberterrorism?

00:04:02  
*Speaker 1:* Plus, uh, the health sector is a good health. To say good is maybe a wrong word, but is an attractive target for both terrorists because it's a matter of life and death. So we can destroy a lot. Um, um, but also, of course, just some criminals because, uh, you have a lot if you're doing it right. Somebody attack. You have a lot to take ransom when it's about people's life. And also when you're doing double extortion and ransomware attacks, you also have a lot of valuable bits so that you need to protect it. So all over this is an interesting fact.

00:04:42  
*Speaker 2:* So how can the technologies like AI and blockchain be leveraged to improve the cyber security in Denmark?

00:04:52  
*Speaker 1:* Um, I think we can use AI. I think there's so many aspects of it again. I think it's important that we're using AI, for example, to detect, um, attacks at an early stage, so we know how so we can actually respond to it. So the early detection, for example by analyzing that traffic or analyze different kinds of activity, correlating different kinds of activities and systems, uh, means that you can detect attack earlier stage. Um, that's definitely one point. Um, but I think the I think responsible use of AI is also important because I sort of opening up many new attack vectors. Do you think so? AI is really a double edged sword. It also has a high value for, um, what's called the attackers.

00:05:49  
*Speaker 2:* Do you see any the differences in the tendencies in the cyber warfare being affected by the geopolitical situation.

00:06:02  
*Speaker 1:* Um, I don't think I see it because I don't have the data for it, and there's some who have done a little bit of research, especially on the situation in Ukraine, but I don't have a lot of data to support it. But of course, of course it's making a difference. For example, when you have a USA that today is saying that they are stopping offensive operations against Russia. There is no doubt that this is giving Russia many new opportunities.

00:06:33  
*Speaker 2:* So what do you see as the biggest cybersecurity challenge Denmark will face in the next 5 to 10 years?

00:06:46  
*Speaker 1:* Okay. At this time, I think it's really, really difficult to predict anything. um, with a political situation that is changing so fast. So I would say that the biggest challenge is to be, is to be ready for the threats that we don't know yet. I don't understand yet. Um, because you're easily preparing for the threats that you're seeing right in front of you, but not, um, but not what you don't know and what you don't expect. So, for example, the move we're seeing now with the US working closely together with Russia, we have the whole discussion. Is the now dangerous, more dangerous than we thought it was to share data with American companies and American authorities. So I think the biggest challenge is in addition to the lack of competencies, uh, and the lack of, uh, management awareness is to be ready for the, for the changing attack picture.

00:07:45  
*Speaker 2:* So what should be Denmark's top priorities to ensure the secure digital future.

00:07:52  
*Speaker 1:* Um, I think competencies and I think securing the small and medium sized companies because they are the ones who can, who have a hard time attracting the right competencies and doing the right things. And they really risk becoming irrelevant when you see companies starting to be more aware of the supply chain and security. So I would point to these two, but of course also securing our critical infrastructure as a country. We are very dependent on our critical infrastructure such as actually working.

00:08:28  
*Speaker 2:* So which I would say advice would you make for the future specialists or people who are trying to get the education in the cybersecurity.

00:08:41  
*Speaker 1:* Threats to it?

00:08:47  
*Speaker 2:* Is there any specific threads they should be looking forward to. Is there any specific skills that they need to have?

00:08:57  
*Speaker 1:* Um, I think we need people with both technical skills and with, uh, more compliance skills, more business skills. So I think we need an approach, a broad skill set in cyber security.

00:09:14  
*Speaker 2:* Do you consider that the cyber intelligence be developed well enough for Denmark to fence itself from the state owned, uh, cyber attacks in the future?

00:09:28  
*Speaker 1:* I think it's always difficult to be prepared enough because you don't know exactly what you have to be prepared against. But but I know that we definitely don't have the level of security that we would like to have.

00:09:43  
*Speaker 2:* I don't have any more questions. Yeah.

00:09:45  
*Speaker 1:* And I really need to run. Um.