00:00:04  
*Speaker 1:* Yep. So do I ask a question and you answer or. Yeah, you just ask.

00:00:08  
*Speaker 2:* You just ask it and, uh, and and and and and no problem.

00:00:15  
*Speaker 1:* So basically I'm more interested in your opinion towards how does the political aspects effect the cyber security and cyber warfare in Denmark. So did you notice any like drastic changes since the Russia-Ukraine war started or for example, the election in the US?

00:00:37  
*Speaker 2:* It does affect us a lot, actually. Uh, the US election, not so much. That's more on a day to day basis. And of course, Trump's rampaging right now is affecting everyone. But, uh, the US election was not a big deal as far in India for our part of it at least. But the Russian Ukrainian war was a big deal because as I liked the Ukraine, We, uh, of course, also target for cyber warfare. And we have seen attacks. Something from Russia and some of them deniable, all from the gas main line to try and figure out who actually blew up, uh, damaged cables, uh, which again, uh, uses Russian, uh, cyber fleet ships, uh, for the more physical damages. But, uh, we are also seeing a lot of attacks. We are seeing attacks on, uh, what? Uh, our water facilities had some Russian attacks recently. We are worried about attacks on a power production. Uh, as for us, again, we had closed access from Ukraine and the access to Ukrainian and Russian websites way back. But, uh, when the invasion started, we decided to block all the known Russian IP addresses and Ukrainian. Not because to like queen, but because Russia is not stupid is the one to blame anyone. That of course try to say, hey, you're creating IP addresses to attack from. And of course we do not expect Washington in section version IPS, but blocking certain countries. We dropped a lot of attacks basically at the moment I think our block list is 47 countries. We don't allow access from all to. And then we open up for some, uh, communication as needed. I actually had a request a few days ago where they asked about some Ukrainian scientists use it. Okay. They could read our data. Of course, we don't mind the Ukrainians. We just don't want every Ukrainian to access our systems. But they actually do. We had issues with Ukrainian working with us and no problem. Russians would be a little more worried about in China, of course. I can say just I think it's we can have a good way to block the new Chinese eyes, Deepsea Eagle, DeepMind and a few other Chinese eyes because the second someone start putting data into them, give it all to the Chinese. And the AI race right now is quite scary because you have no clue what's going to happen and what data they steal, and people do not think before they put data into AI, but because they are friends. No they're not. This team will get.

00:03:29  
*Speaker 1:* So so basically, which law would be like beneficial to introduce to kind of protect the citizens and the users of the like for example like AI systems and like just a I would say like how to secure companies maybe. Is there like something.

00:03:48  
*Speaker 2:* For AI also the European Union will have to do some general, uh, law decisions about how to handle ice in European Union? I don't think that should be on a country basis. That'll have to be European Union deciding, and that takes a while. It's going to take years, probably. What we can do, of course we'll do some floggings on a on a country scale. For example, we had a massive problem with the Chinese cameras because they might have backdoors. And I think most of every government functions Denmark are not allowing, uh, efficient Chinese cameras and probably others. But again, that should be probably a European decision for EEA. It will be for more. Smaller things will be country based of course. No laws against here. Don't attack our power production. Water production also applies, but I don't think you have to make new laws in that one to protect us because the attackers don't care about the laws. We just need to. We just say, don't do it.

00:05:00  
*Speaker 1:* Hmm. Interesting. But would you say, is it like there is a definition between, like, the victimology in the cyber attack? Do people usually target women or men, or is there a specific race that subjects the cyber attacks more, for example, like the.

00:05:19  
*Speaker 2:* Oh, yeah. Go on. Sorry. Go on.

00:05:22  
*Speaker 1:* Oh, no. It's fine. You can, you can, you can go.

00:05:25  
*Speaker 2:* It depends on the attack. If it's the normal. Hey, I'm a Nigerian prince. I have some money for you. It doesn't matter. But attacks attack on men or women, depending on the type of attack and what they want to do. If they want money for men, we'll take by the usual. Hey, I have big breasts. I'm in the bikini. Uh, want to talk to me? If it's women. Uh, we could make a target by the love scams And it said effective. I think last year I think it showed the numbers they got around to. I think it was 17 million, uh, of Denmark in 2023, full of schemes alone. And those are mainly, uh, attacking against the women, uh, the attacks in regards to blackmail about what people are doing, which usually target men saying, hey, I recorded what is in PC, uh, or even worse, they actually it's not a bluff, but they talk to a nice woman that's turned out to be not so nice. That used to be a targeted attack on men. I assume, and I'm guessing here, but I have from news, I think it looks like the. You would probably use a battlezone like Ukraine. You'd probably use stabilizing attacks against mainly women because the wins in the war. And if you can start saying, hey, how about we attack the women, sent them emails to the house goons and show them pics of their children. So on to to demoralize the population. And because the men are usually the ones fighting, that would mean to be targeted against women.

00:07:05  
*Speaker 1:* Mhm. What about the children for example, like uh, usually cyber protectors, they target for example hospitals. One of the reasons could be like the amount of patients and to create like disturbance in this society. What do you say about that. So what is the main reason in attacking like the hospitals and critical infrastructures. Is it because of like the terror and like I would say like to scare off people from using it and like.

00:07:36  
*Speaker 2:* What we have seen in hospitals is, uh, so far as I what I've seen, I've only been a ransom money based ransomware attacks originally, uh, the criminals figured out that I suppose it is a bad idea to target, and that last until, I think three years ago, because hospitals were only targeted as collateral damage. Because you said now to 200 million, 200,000 people and some of them are nurses. Uh, and, uh, I know the European Union attack, and Interpol is going quite hard against people who take hospitals. Those incidents from years ago with the attacked, uh, German hospital by accident. They're supposed to take the local, uh, college or university, but the same thing with spittle. And a woman died during the transfer to another hospital. And Interpol, uh, clearly told the press that this is not a random attack. This is investigated as manslaughter because a quite different, uh, penalty of law. Just so you don't target hospitals. That has changed because people are now going and don't care direction for the, uh, for the hackers. They just want the first case. But that's the ransomware part. I assume that if, for example, Russia or China would really bother us have that would be a target. It'll be more beneficial to target, uh, power plants, water infrastructure because that also hit everyone, not just hospitals. But we would be a target, could be a target. As for blackmail. That'll probably more interesting for most countries, because can we steal health information? Can we use to blackmail someone in the US? They use it for, uh, insurance fraud because, hey, it cost half 1 million USD to get treated for cancer. If we had team identity perfect in Denmark. Free healthcare. That's not that interesting. That's more about the blackmail. Or can I use this in other ways? As for children, I have not heard about anyone targeting children specifically. I would probably say most people wouldn't do that, but of course, if someone in a children's ward click in the wrong email, it'll have also hit the second ward. But I've not heard about targeted attacks for children. And then we're actually more focused about, uh, influences targeting children for. Advertisement. That caused a problem. The press once in a while.

00:10:10  
*Speaker 1:* Okay. So what impact has the Ukraine conflict had on NATO's cyber security policies and international cooperation?

00:10:21  
*Speaker 2:* We have, uh, and we've stood quite, uh, united against Russia. Uh, and since Russia happened to really enjoy doing cyber tech or hybrid warfare in this country, there are a lot. Ukraine have had to pull cyber security because we all targets. Denmark is more of a target because we have supporters with quite a lot of money person wise compared to other countries, but we all targets, uh. European Union has done all the list work to do a block against the Ukrainian fund. Russia funding again, have confiscated Russian holdings and what we have been able to do, I call that love. That is, uh, cyber based. So here we we are now basically stealing your account because you're stupid enough to target a country where we allow to put your money in our banks. But yes, we've all had to impress and prove our cyber security. And we consider again Russia. But I think most countries, most companies Denmark right now is saying, hey, maybe we should reconsider. Can Russia, it even hit us. Should we worry about Russia? What what can we do? We've done what we can by blocking them. And, uh, generally trying to tell our employees that, hey, think about what you're doing.

00:11:48  
*Speaker 1:* So basically, what lessons can other nations learn from Ukraine? Cyber defense strategies. Did you learn something like from, for example, like the cyber warfare that is going on between Russia and Ukraine since there has been a incident? I believe it was last year regarding the mobile network that was down for a couple of days and people couldn't make the calls to the doctor, they couldn't access any like private institutions and get any information.

00:12:23  
*Speaker 2:* I don't see from my end. We have not learned much from your cyber defense, because what you're talking about here is not cyber threats as such. It is attacking the infrastructure. Of course, we didn't say, hey, let's have backup systems, uh, have generators in case we lose power, have water supplies. Uh, but This is more on a fiscal basis. Again, our government has said, hey, maybe we should prepare people to say, hey, make sure you have food or water for three days, which we have a radio and so on, just in case. The same would happen here because it can happen. Personally, I would be just as worried about an old ransomware attack then Russia taking that regard. But yes, it could happen. And but that's more physical. I have no clue what Ukrainians are doing in regards to cyber protection. So I can't really talk about that one.

00:13:18  
*Speaker 1:* Okay. So basically, how would you say that the political stance effect the cyber warfare in Denmark? So basically what what is your opinion about like that like Danish cyber security, since it was um, the level of the cyber security risk I guess was raised from a low to medium. In June 2024. So can you give any comments about the recent cyber activity?

00:13:53  
*Speaker 2:* The fun part. It hasn't changed much for us because, uh, there you were referring to the set of security, uh, warnings and those in regards to our sector actually being high to very high for years before the conflict. It has not really changed for us because when you order at the highest level, okay, Russia invaded. And can you increase it? No we can't. We are on the maximum level already. So the official designation has not changed for us, but the focus from the past position has changed again. Four years ago we had two people with toner in the security department here. Uh, we have upscaled and our politicians have noticed that cyber attacks is a problem. Security is a problem. They're putting money into it and everyone is doing that. Not just hospital sector. Everyone is putting massive money to cyber security. And no, Russia is not the only one. I'll say the pressure from China is also a problem for us as infrastructure and attacks for companies. It will probably more be in regards to cyber security about Chinese copying or damaging attacks.

00:15:07  
*Speaker 1:* Okay. How would you how would you describe more about the for example, how does conflict in Asian countries affect the stability in the whole world? Since there is a lot of conflict between the China and Taiwan and China and the US, China, Russia. So how does it affect the whole world? Since you mentioned that China tries to copy the ransomware in order to infiltrate.

00:15:37  
*Speaker 2:* It affects us greatly, actually, because there's a lot of interesting countries in that regard. North Korea, uh, due to all the, uh, embargo against them, they basically only get outside money from cyber warfare, and they have a lot of good people doing it. They are mainly focusing on, uh, attacks on the East Asian countries that do a lot of attacks on ATM machines in Asian countries, saying he wouldn't get a half 1 million USD out from ATM machines during one night. Perfect. So they don't run that one. Uh, they're doing some attacks, but nothing big. Uh, China, on the other hand, they're problem because they're trying to partly support Russia. They kind of bang out a little bit. North Korea is giving, uh, soldiers to the Russians. I'm not surprised they can will pay, probably because they need money. But China is kind of a half and half saying we might support Russia, but they also read back over a moment's notice if they don't want to. But on the other hand, if the US managed to peace treaty saying, hey, Ukraine lost the lead, they got Russia's backing off. Now, like Trump said yesterday, uh, in that regard, we are sending a clear signal to China saying, hey, go to Taiwan. No one cares. So basically what Russia's doing. Well, if the US backs out and NATO backs out, uh, a large contingent will say, hey, let's take what we want. The US included, considering from now, right now on Canada, but the Panama Canal. Uh, Greenland, uh, and, uh, basically charging through whatever. They don't like it at any given time. The case has to be also on that one. So, yeah, uh, every country, big country right now saying, what can we steal? And, uh, in Asia. China will take Taiwan if they allow to, they will also bother. The Philippines will take some of their land if they've allowed to. And the impression that, of course they don't. They need more land, basically. Uh.

00:17:46  
*Speaker 1:* Yeah. So so basically, you're saying that the stronger the need goes, the stronger it will be. The danger from Russia, China cooperating together and creating some new ways of attacking. But what will be like the reason for the attacks? What will be like the reason behind all this? Like crime, I would say like, is it like the income, the ransomware? I don't know what what do you think.

00:18:14  
*Speaker 2:* For North Korea, for North Korea, it's money for Russia, its land, power, prestige. Because, uh, Putin wants to recreate the old, uh, uses ah, he wants more land. He wants all the old and Russian, uh, countries for China. It's, uh, money. Not in regards to money from cybercrime, but the intellectual property, they don't care about that. They want to copy whatever they can get their hands on. So can they steal, for example, a new. If we're doing research on HQ and we can still let them produce it, perfect for them. It's money in regards to intellectual property.

00:18:52  
*Speaker 1:* Oh.

00:18:53  
*Speaker 2:* But but again, if they can do some more destabilisation along the way, it'll increase their chances if NATO falls apart. If rush backs out. The EU's already left the Paris climate treaty. They threaten to leave NATO, whatever they use based out of weakness. Everyone. And it will sell to both Russia and China that I think are now stronger. Go ahead. So yes, if they can also affect saying, hey, we can affect public opinion. Let's, for example, say there's an election in Germany coming soon if they can get the the right wing alternative for Deutschland uh kicked the more popular by doing false news and, uh, misinformation campaigns. They will do it because it'll increase their chances, because that means they will be more likely to not support other countries, including the Ukraine, but also not backing up later.

00:19:48  
*Speaker 1:* So basically, you're saying that if the NATO will start falling apart, there will be like a power struggle and there will be the, I would say, like money struggle between the countries who want to infiltrate right now. But basically, how will they unite based on what will it be the most like political issue, or will it be the issue of the interest so everyone gets it won't.

00:20:19  
*Speaker 2:* Russia, if it falls apart, Russia will, uh, at the minimum, try to reclaim all of the users are countries that for the Soviet Union fell apart. That's Putin's dream. So yes, if nature drops, he will go for that. He might be limited because he just loved Ukraine, killed a lot of soldiers. He lost a lot of manpower. He will not have manpower to actually start doing that. But North Korea, just 10,000 soldiers. Uh, China had 1 million people. One of the largest ministers in the world. If they can, if Russia can rent Chinese soldiers to do his invasion, perfect his manpower enough for no one to stop it, basically. China will most likely not start to invade anything there because they'll have to, uh, invade Siberia, which will counter intuitive by supporting the Russians. Or they have school after some of the what? India and Pakistan, which both have nuclear weapons thus probably won't do it, but they will extend the other direction saying hey, Philippines, Malaysia that that way. But Russia will probably be the big land spreader.

00:21:32  
*Speaker 1:* All right.

00:21:33  
*Speaker 2:* So again some good news.

00:21:38  
*Speaker 1:* So basically you mentioned the election in Germany. So can we speak about more about the how does political stance over not Danish, not Denmark, but basically like what is the consequences of different like ruler ships in different countries can affect Denmark. So for example like right now Trump came to the power and for example, his political decision was to propose to buy Greenland. So how does it affect Denmark and Danish Danish security in general?

00:22:15  
*Speaker 2:* It affects greatly because whenever one continent make a stupid decision, it'll affect all of us. Right now, Germany is talking about a again, putting in board control, which means everyone, uh, working, leaving Denmark, Germany the other way around will now have massive increased travel time. To be fair, we did the same a few years ago during the Syrian war. We had a lot of refugees and, uh, our own would like to have border controls back, but that'll affect us. Border control suite would affect us. If, uh, it doesn't get more power in Germany, they will start to say, hey, we don't like foreigners. Uh, we don't like asylum seekers. What should we do then? That they will try to affect you saying, hey, somebody else need to take all the foreigners and that will stick out in my hand. The foreigners? How? Everyone will do it. Uh, we have people like, uh, Erdogan in Turkey who basically, whenever he wants to try to blackmail Europe and say, hey, I'm part of the European Union, I don't care. But if you don't support me, give me some money. I'm just opening the gates and letting all the refugees in the Europe. Problem solved. So yes, even European Union countries are doing problem like problems like that. And if some of the more, uh, Eastern European countries in the European Union, uh, will start to look more to Russia that also affected because they will start the collapse of the European Union. If people start leaving, you can look at England, the the positive side after England left the European Union, uh, they the cards were just shit. Uh, they kind of tanked, uh, everything. You got to give me a problem. That's been a wake up call for everyone else, at least. Uh, before that, there was also a lot of people in Denmark saying, hey, we should leave the European Union. That discussion stopped around the months after England did because we saw what happened. But again, if Russia can try to fix public opinion and say the opinion is bad and do misinformation, it might affect some people and they would.

00:24:26  
*Speaker 1:* So basically you mentioned that. Eric Holder speaking correctly. So basically if the population will be kind of like brainwashed, so is it easier to control the nation and the world? So basically how would like how will you comment the situation right now in Russia that they don't have really much the access to the outer world, and therefore they are locked in their own bubble?

00:25:00  
*Speaker 2:* That is a problem because again, it's control information. You control the population. Russia is a good example. Russia, to be fair, do have some access. They do allow instant access. They're not locked off. They are more locked in the regard that if people complain they have to fall out a window. And basically there was some musician that fell out a window two days ago after what happened. Happens. Uh, but, uh, countries like North Korea, for example. Uh, they don't allow their citizens to have access to for me. They are they are completely in a bubble. In that regards, the only way the people be able to do anything is by rebellion. And, uh, since the military is run by the the government that don't have money to let the military decide what happens. Um, in Russia, they would probably be, uh, yeah, if we saw the groups that try to be something like that one, because they basically said, hey, we don't like what you do and actually start moving towards Moscow with Halfway to Moscow. That one's got them scared, because what if one of the other countries do that? Then what happens? Which means the government should try to rely on, uh, military power and suppressing the population like Russia too. They need to be very careful. The military, they don't need to be scared about the general population because they don't have arms. They're not armed. They can't do much. I'm not sure about the general Russian population, whatever the arms they have. I'm pretty sure that any military is just a military. Probably still in Denmark. We don't have access to arms. If our government decided to say, hey, let's do dictatorship and put in the military, we couldn't do anything. We don't have a weapons. The US will start a civil war because everyone has weapons. So we can't. Depends on the country. But yes, if you can block the government, the people from getting reliable news or effect and use to a certain degree, it'll be a problem. A good example is the Philippines, where my wife is from. Um, they had uh oh. What was their names, too? Uh, two seconds. Uh. Uh. Uh, Marcus, the Marcus family in the Philippines. They, uh, went to take a trip to the Philippines. They had martial law running for 20 years. Uh, they got killed. Come to this over 15 billion USD. Uh, on the way out. Um, then again, because they managed to quit the, uh, misinformation campaign because most of the Philippines don't have that much money. Uh, the general population, uh, will have access to the internet. They won't be able to afford good institutions, so they get access to very limited, uh, mobile phones and where they get access for free. But they if they use Facebook and Messenger, they basically use Messenger and Facebook and when you can then make sure that what pops up on Facebook is Marcus, then people believe it. The general, uh uh, teenager in the Philippines thinking that the Marcus family did a great thing. They don't think they had military law. Uh, military total of 27 years. Don't believe it because Facebook says so. This is an amazing campaign hiding what actually happened. It takes around five minutes on Wikipedia to read what actually happened. And see, that's probably not a good day to vote in again. But they managed to hide that and it worked.

00:28:53  
*Speaker 1:* So how would you commend the effect of Facebook and other social medias on population?

00:29:01  
*Speaker 2:* It's big. It's very big. And uh, with the current, uh, policy climate in the US, where the Trump and the tech media is basically gathered, uh, together and Trump is doing weekly, hey, what are you allowed to do this week thing? It's a problem because right now even Musk's the Twitter basically say, hey, if we don't want something on it, we don't care. Uh, last week there was one media, one government agency who was not only allowed to public announcements on X perfect, but now control what they're saying. Trump is doing that. Uh, in Italy during Berlusconi, you had the same situation where he owned all the TV stations which chose not to report. And the U.S. is going that way right now is the more you can affect the media, the worse Denmark. You see, people complain all the time about how we don't do how are we this biased? I don't think we're that bad. There are some laws saying, hey, you basically have to not lie. Of course, we all see how how deep we dig when researching a story, but in general we have not biased media in Denmark. Uh, if you if you're you think I'm reading the code from that on a website for right wing, that's probably good news. But if you go to print the newspapers, you are generally okay. Of course, except that it is more clickbait than anything, but most of the serious newspapers will do okay. Most of the online or TV based news is doing okay, but it can't be a fake. And if politicians can start influencing what you are to report, it's a problem. And social media makes it so easy to cause people lost. Critical sense. People don't fact check. That's a big deal if you don't fact check your fact. And Russia's abusing that right now.

00:31:00  
*Speaker 1:* So basically, how does it interfere with cyber warfare? Is it one way of criminals to contact the society or one way of manipulating?

00:31:11  
*Speaker 2:* It's not it's not affecting cyber Cyberwarfare. There's more disinformation campaigns to affect public opinion. Uh, criminals are abusing it somehow, uh, in some way to, uh, try to steal money because he, uh, Trump said something stupid, click his website to see it. But, uh, in general there too, the old fashioned way, in case the criminals wouldn't, uh, have much issue doing that. A little more big country based attack or information campaigns. But of course, if a criminal gang would have a political influence, it depends on the definition of criminal gangs, actually, because Russians, uh, they don't do hack Russia, don't do cyber warfare. They, they have the criminal gangs doing it for them. Technically, I don't think rush the Russian state too much cyber warfare. They just use groups that have. So if you define those groups as cyber criminals, then yes, they do a massive amount of information, but it is state sponsored and state owned in practice.

00:32:17  
*Speaker 1:* You mentioned right now about the state owned cyber groups. Are there any existing in Denmark?

00:32:26  
*Speaker 2:* Take the new, uh, in practice a little bit because, uh, our, uh, uh, fee for source in front of the CCA, basically, and our army internal are recruiting, uh, cyberwarfare, uh, people. We had, uh, one completely stupid position. Let me just find it. A few years ago, we had a. Default position who, uh, basically went in the press and said, uh, yeah, I didn't actually start doing cyber attacks. And we get attacked because we have are so great in cyber defense. And that's basically just saying to the hackers, hey, let's test that perfect system. Not a think it was, um. Uh. I think was trying the bombs to deter. But basically she said to the hackers, hey, we're great. We are we are part of the world. We're doing. You can't get in. And of course, that increased the attacks a bit. But yes, our army is, uh, doing, doing, uh, recruiting. And of course we should, because we need some people set up a cyber second is also, of course, having both, uh, red and blue team techs in our department. We also need to be able to say what will happen if we attack. We don't attack anyone, but, uh, we defend. But I'm pretty sure some of our, uh, army will be doing some attacking also. Not in a big way. But I will say if you find out if you have something like, hey, the Russian are using, uh, some health service in Holland, for example, if people can trace those to Holland and, uh, put down the service or get the Holland police to do it is taking an attack to defend ourselves from attacks. So you would in that way say you have two cyber attacks. But they're not as inherently take on power plants in Russia. In Russia, no, but you do to take down criminal gangs and there they attack vectors.

00:34:51  
*Speaker 1:* Okay. So you mentioned the gang. Gang, uh, cyber gangs in Denmark. Do you have any members in Chip who can help with the cyber attack or cyber defense? So who is the main people in Chip who take care of it.

00:35:10  
*Speaker 2:* I don't think you have any, uh, the best probable data. Uh, and, uh, he's not doing security. He basically don't want to be in our department. Ask him, he said, and he knows himself, and that's good. I'm going to be too paranoid. Perfect. Then you shouldn't be there. Because if you're not paranoid, you shouldn't be in our department. So I don't think you have any. You. You rely on us to do it. Uh. And I would also be very afraid if I was, of course. General information. Teaching your own staff, saying, hey, be a lookout. Be reasonable to try not to do anything. But, uh, one of the things we look for, if you if one of our random doctors or nurses or whatever. Start playing around with the hacker tools. We get noticed and we talk to them. At the moment, we're trying, we're trying. And you cannot go into this one. But we actually starting to Working on a few plans to see if you run a hacker through the machine. We isolated the machines cut off from the internet until we talk to you, because we don't. You're not allowed to do that. Even people in my on my floor who might work as a windows thermostat, if he's using a hacker tool, we can talk to him. Say why? Because he's not allowed to. He's not supposed to do that. There's good reason we can discuss. Otherwise, we cut them off. We had example. Again, you're not allowed to call this one yesterday, uh, where we saw one of our medical systems, uh, using PowerShell script to take screenshots. And our suppliers only have all their data. It's in Houston, their servers, so that they need to take screenshots of potentially extensive patient data. That'll be illegal. Uh, so I called to, uh, to, uh, for our one chance of the system down, said, hey, what's going on? Because if you don't know what's going on, then we need to talk to our IT worked with department and lawyers and turned out that they knew it, because there's one of our doctors who was doing some checking about errors, and along with collecting the logs to take a screenshot to see how the screen looked. And we had to say, that's no good. And that's also going to be blocked. If you will do that, they can isolate it. So we really don't want people apart from us doing it.

00:37:30  
*Speaker 1:* So who are the first people. Yeah.

00:37:35  
*Speaker 2:* No go ahead.

00:37:36  
*Speaker 1:* Yeah. So basically who are the first responders to the cyber attack? Who is the first wave of emergency response team?

00:37:44  
*Speaker 2:* In our case, it'll be our SOC, which means our best to the one who's doing 24/7 surveillance, the, uh, getting alerts. So somebody calls and say, hey, you have a problem. There's problem with general it with them getting the call, and then they talk to us during daytime hours. Uh, we just, uh, stopped our having a 24 over seven call duty. which means that if no one is is after 4 p.m., then, uh, if it's not important enough, it'll. Which next morning is another trigger person here to try to call around and see if anyone is interested in helping. Uh, but we don't have a 24 seven call due to their said.

00:38:24  
*Speaker 1:* Were there any recent cyber attacks at a hospital?

00:38:33  
*Speaker 2:* Um, no. Uh, the attacks that's going on all the time. We block, we get those all the time, they get blocked all the time. We, of course, have all the normal, uh, attacks as a scam, phishing and so on. But we have not had any big attacks affecting anything quite a while. Obviously, when I started with defining a big attack, as in something recently, this town, we haven't seen anything in years. Uh, back in 2018 was the last time.

00:39:05  
*Speaker 1:* Can you?

00:39:05  
*Speaker 2:* When I start. When we start the region, what we have called this game. Which means we are in emergency room. Even in the intervention. There we are. There we are talking about what you tell the press. But we started the region with those every week. We are two. Last year we proved quite a bit and there was not cyber attacks, but also something went down. Uh, center for folks who don't have power rooms, everything's down, stuff like that. And we don't have that much of that anymore. Um, data attacks, the last few ones we had where we actually felt something for status attacks because they managed to use some new techniques that they basically flood our router so we couldn't connect to anything. We had 30 minutes of problems and traffic from outside Denmark cut. Problem solved. And then we fixed it and started up again. But we haven't had anything in well over half a year. Uh, and the data takes the only thing I can remember in Government recent time.

00:40:05  
*Speaker 1:* Can you enclose more about the major cyber attacks that were in your career? So you mentioned the 2018 accident.

00:40:14  
*Speaker 2:* Yeah. We yeah.

00:40:15  
*Speaker 1:* And I would say it was not big attack. It was basic ransomware. Our problem was our enterprise was not good enough the time to take it. Uh, and our nurses and doctors basically went through what it was that made us click on it. No matter what we said, no matter how much warned. And if we had. Yeah. From 15 to 17, uh, we were attacked every week. We had, uh, me and my boss has. We would be restoring data. The virus circulates. You do? When someone checks, uh, what they did in the old days, antivirus was. Hey, is that dangerous? Yes. No, it's a new file. We don't know it, so it's probably fine. Uh, then the whole enterprise built in ransomware section something. He is someone trying to to increase encrypted a lot of files or touch a lot of files really fast. That's probably not a good idea. Copy that process that solves it. And we have not had a ransomware attack since, and we have not really have any big cyber attacks apart from that.

00:41:18  
*Speaker 2:* So what what were the key components of the emergency response plan? If you can enclose it, of course.

00:41:27  
*Speaker 1:* Uh.

00:41:28  
*Speaker 2:* Basically, I think you have it already because you got a copy of the basic plane. Uh, this one was on The Sims two last time. Basically following that and saying, hey, this is what we are handling. We are sitting in one of our rooms, have all the important people in, which means all from press is bad enough to tell the press we're down. Uh, we have some form of communication. We have our directors, my department. Uh, any other relevant department? If there's patients treatment, and you'll have representatives from the department to coordinate and sell the tools that they need to use emergency procedures and so on. And basically one track is a technical one where we're trying to stop the damage, find out what happened and how to restore. But a lot of stress is informing the press, informing our users, and doing emergency, uh, routines so people can work. Because if something is down, of course, we don't really stop treating patients. There would be mostly procedures in place for basically everything. Of course, if there's no power on Earth, because, uh, Russia took over a power plant, we have to evacuate patients. Uh, but if there's generators, how how much can run? Before we were actually patients when we op that's important part thing when it comes to work, you can start working with evacuate.

00:42:57  
*Speaker 1:* So basically you mentioned about the patient's risk of being kind of a victim of cyber attack on the hospital. Can we talk about the bespoke hospital incident?

00:43:12  
*Speaker 2:* Yeah. Which one?

00:43:14  
*Speaker 1:* I think you mentioned it the last time that some couple of years ago, there was an incident with the medical equipment in the hospital.

00:43:24  
*Speaker 2:* There's no. But yeah, the that ransomware is where one of the hospitals, uh, you probably shouldn't mention the hospital, but if you're doing you purchased the er, hospital, but, uh, yeah, one of our hospitals, uh, one of our doctors had basically just share my screen. Two seconds.

00:43:44  
*Speaker 1:* Yep.

00:43:45  
*Speaker 2:* Um.

00:43:49  
*Speaker 1:* There we go.

00:43:49  
*Speaker 2:* Very, very simple. Uh, what he did was just like I'm doing here. I'm doing a, uh. I'm seeing someone who loves MapReduce because it's a shortcut to my own path. It's easy, it's nice, and when you can hit a ransomware, it's all said what you have, what you have here. I'm not just looking through all the drives down here. I'm also saying, do you have something mapped here? And he had a connection to Azure on two servers where we had all the results of a blood analysis. So the last day of the blood encrypted, we could restore it. Problem solved. But, um, he fucked up the cost of the server while we restored SMB. That's the biggest impact I've seen on, uh, patient information. There was nothing lost. No problem is just we had a time where we were not able to do blood analysis and to restore the results we already had.

00:44:46  
*Speaker 1:* Yeah.

00:44:47  
*Speaker 2:* We have logged. Not have anything bigger than that. Okay, so it will come. It will be there. But you haven't seen anything bigger.

00:44:55  
*Speaker 1:* So basically, the consequences of this attack was not to damage the record. Not to.

00:45:03  
*Speaker 2:* No. Okay.

00:45:05  
*Speaker 1:* What what what what happened was that, uh, when you when you go outside, you can see blood taken for analysis that would be run through some machines to do whatever analysis you need to do. And the results of those were, uh, encrypted. We could restore them. Uh, no problem. But it meant that we had to, uh, stop analyzing the meantime because we had to turn off access to those drives to restore. So they had to, uh, restore the results manually on the machines and not upload to the server while this was going on, so we could still do bloodwork. We was just slower, and we had to do some extra work after to make sure everything was okay. And the results we had done, we had to restore in the meantime was that this was any really important bloodwork and say, hey, we need this now. They still had the samples. They could do it again. So we do not have anything. Where? Here. The patient can't get treatment because we don't know what happened. No. We might spend an hour doing the blood work again, but it was too possible to do it all. So there's nothing lost.

00:46:10  
*Speaker 2:* Were there any more incidents like that?

00:46:15  
*Speaker 1:* None I'm aware of. We've been lucky, to be honest. We've been lucky. It will happen someday again. We are open. We have 50,000 users. Half of them don't know how to do basic security. You can never think something will happen someday. No matter how could we are. It will happen. The question is, how do we handle it? How will I prepare to do emergency procedures? And then we train those yearly in out in CMC. But most of the departments should also do emergency training on how they handle it. Sadly, they don't always do it. My wife and her department. Uh, they had to do it recently, and they, uh, they have a lot of physical problems that say, hey, if something's down, we need to have physical copies of a lot of materials in storage, just in case. And turned out that basically everything in their emergency box was out of date and end of life, so I couldn't actually use it. So they figure out, hey, we need to maybe we need to order some more and have procedures saying, hey, every six months we might need to replace what's in this box, stuff like that. And a lot of parts will not have properly under control, but that is an IT problem. There's a host department problem. So we we can tell them make sure you have that control but we can't force them.

00:47:40  
*Speaker 2:* So basically you mentioned that there is a yearly trainings. So is there like a better way to prevent that. People will click on link that they don't know, for example like raise social awareness. So how to react on the cyber attack. So basically a lot of people nowadays are getting hacked on Facebook and different social medias, and therefore they fall into the panic and don't know what to do. So what would you advise to do in this stage?

00:48:10  
*Speaker 1:* What we do. The important part is, uh, educating the people. Do awareness training. Uh, we are doing it every year. You've probably had. You should have done it. At least is required IT security course here too. Every year we make new course every year. Uh, and we don't have enough resources to do it. That is not a request. But what we can do is question what we allowed to do. Uh, at the moment, it's basically saying, what? How much time do we use versus how many patients can could you treat that time? We are allowed to use 40 minutes a year of people's time on awareness training for ten minutes. The problem is with 5000 people, if you say, hey, let's use one hour, that it is 50,000 man hours lost every year. How many percent of that? Can we justify that? And we can't. But that is a decision from the rulers, our top political bosses. We have to decide if we can force it. We've. Every time we hire a new person in my department within a month and say, why don't we do a phishing scam, phishing awareness training? We can do it. I tell my players, I know how to do it. My education told me how, yes, it's easy. It's not a problem to send an email out to people. The problem is, if we're nice now, we're talking very nice. We are saying we're not doing a full phishing campaign, uh, awareness campaign. We are doing a small campaign time. 5000 people. That's under 10% of our employees. Just 5000. We've been very nice. Half of them don't pursue them or don't bother because many of our employees don't read meters. My wife's had three in his first month as the cleaning staff. They don't get in, read emails. They get information about buses. They would never touch the mail. We have a lot of accounts, never open their emails. So let's say we have 2500 people to see them. We'll have to see 2000 of them. See I don't care. Delete. Perfect. Then we have 500 people who are worried, and they call our helpdesk to ask what's happening. Then we have 500 people in one day in a cube on our helpdesk, which also get all the normal request, which means that an actual problem from a nurse somewhere would have to have her in a two hour queue to get help. Of course, that could be fixed by just saying, hey, some more people should be at work. Yes of course, but I'll helpdesk. Is the staff the bare minimum? We rely heavily on the temperatures. Temperatures take a few months to train at least, which means we have kind of a wave thing. We say, hey, our, uh, uh, caseload is doing like this. When you get up here, we have a problem, then we have to focus. Then it goes up coaching tempo. But when they're done training, it falls. Because now with people that handle it with bounce, normally we find the temperatures and we have a cyclist doing like this, which means that we need three months in advance of doing efficiency, and the 5000 people need to hire workers and train them. That's not going to happen. I would like to, but we can't do it that we need political, uh, agreement that we can't get policing to do.

00:51:31  
*Speaker 2:* So I wanted to ask you, is there like any, like, threat hunting reports that can be used in my bachelor thesis? If there are any, we produce.

00:51:44  
*Speaker 1:* No, no, I'm allowed to give you a sorry to see because they will really relieve a lot of our internal problems. So then, then our public, um. We would not even be allowed to leave. We had our, uh, exercise. Yeah. Sorry. Yeah. They, uh, that would, uh, massively issue where our problems. Because we have to where we are way behind we all behind medical medical devices are way behind. We have loaded system. Which means any reporter saying here, here's our weaknesses in a public report would be exploit could be exploited. So I can't give those out. But we are doing the checks and we are aware of them. And we are trying hard to fix what we can. We can't fix everything. Uh, the example, uh, Liz Taylor is doing buying, uh, pressure chamber, uh, you know, timing sickness. That sounds true, because why would you have that? Doesn't matter much. We have location driving extent, but it also turns out that, uh, wound healing is improved by being under pressure. So we actually have some people with the difficult wounds who would a few hours a week is going those pressure tanks with oxygen masks to help on the healing. One of those, uh, chambers, they don't get replaced every few years just because it changes. But less than 30 or 40 years, they want Windows 11. That's fine. But that is in the 5 in 10 years. What to do next? 20 years? We have that one. We don't know because you don't know because they can't buy always. That has a lifetime 30 years. Which means we need to fight. What can we do in that time. And all those little problems is too big for us. And, uh, we do what we can, but we can't fix set can fix everything.

00:53:40  
*Speaker 2:* So basically what you're saying is that outdated software and outdated, for example, like medical equipment that, for example, has the, I don't know, outdated lines license is a threat analysis license.

00:53:56  
*Speaker 1:* Both license but also, uh, technical support because a license would say would just imply that we are under license and we probably could get fined by the supplier. But when you can't when you run windows XP and you can't operate, uh, then you got a problem. We had a they fixed the now luckily, but we had one machine, one with XP, which has been in the flies over ten years. But, uh, she was uh, by, uh, EU requirements, uh, supposed to run it because she was part of a research team looking into, uh, genealogy and the inheriting diseases and the software they used to used to. Family trees had to be the specific software, which was last updated in 1999 and could only 116. And that is a new requirement. We couldn't fix anything. We had to give her next machine. And as long as we have that, we can't do anything. The medical industry is getting better, but they are waking up from a 30 years of we don't care. And it took years to fix it. And all the other stuff we have is a problem. We can't just go out and I'm going out and saying, we have probably ought to have 2000 medical devices in the in Houston. And we don't know what they are, how they're running. We might not know who's responsible for them. And we don't have the money to upgrade to version if that even exists. And all of those are potential attack vectors. And that's a big problem because if one wants a new thing, it wants everything should be in Wi-Fi. Yeah. The problem is thinking you can read something. You have a potential weakness. Some of the similar saying. Hey, peacemaker. Yeah. Hey, if it's Wi-Fi. It came as a data to our servers and say, hey, it's been doing okay. He commands the treatment. Is the peacemaker okay? This is great information, but also means I can take it and maybe affect how to affect the heart. Turn it off. How do you patch a pacemaker? I have no clue. I don't know if you can. And we can do security scans on the pacemaker. Stuff like that is the problem.

00:56:15  
*Speaker 2:* So basically, for example, like if someone gets a heart implant, I'm not sure how it's properly monitored, but probably it can be connected somehow wirelessly. Is there a risk of, uh, for example, like shred for people getting access for the medical equipment that is.

00:56:35  
*Speaker 1:* I have not heard of any attacks like that, But it is a potential risk. And this question, honestly, of time is not worldwide. And there's probably have been some somewhere. But, uh, let's say a simple thing. Uh, I have a sleep apnea, which means I use a CPAp machine. That one is, uh, have a built in so they can fall back to the hospital. Potentially. That could be hacked. Uh, if someone were to adjust the airflow on my CPAp machine, it could potentially affect how I sleep. Uh, sleep apnea can lead to heart problems and can lead to heart attacks, which would I could potentially risk if someone were to do that. I've not heard of anything doing it, but it would not be impossible to do. And that's the problem for it is cuz it's not saying he would likely. It's also say he. If it is possible, we need to try to protect it because unlikely don't mean save. Just mean someone have to figure out how to exploit it yet. But I could see an Asus issue the second. Uh. What should we say? A good example is what I just showed here. It's okay to blow up a fetus. What happened when a terror group figured out that the most common hearing aid, which is now also online and controlled by a specific company, whether they can extrude those or get malfunction, get them to a massive sound to damage items and use that to say, hey, we need money or we can attack all the customers. It's not unlike this scenario. It'll be hard, but it's going to happen someday. Stuff like that will happen. We've not seen it, but it will happen. Yes. And the security solo on it that we space stuff like infusion pumps, for example. It's always a good time because those are so insecure institute that can't remove it.

00:58:38  
*Speaker 2:* So should I mention it in my project or should it be better left out?

00:58:46  
*Speaker 1:* No. You welcome to mention of medical device because that is a big risk. Uh, Google medical devices and you will have the first 200 pages. You can read about it. There's no big deal. Let's see. Um, and, um. That is normal.

00:59:06  
*Speaker 2:* Okay. Yeah. Since I want to ask you also about the.

00:59:10  
*Speaker 1:* It would be basically when you have, um, when you're talking about hospital and focus on hospitals, it is something you should have a report a simple now just need did a very simple research saying, hey, unsecured medical devices. Yeah, yeah. You can see here's all the food first to the Google. It is well documented and it is not been fixed since. There's a lot of it.

00:59:37  
*Speaker 2:* So what? What is your kind of like opinion? What is your technical opinion on the situation? When the pagers were blown out, the terroristic attack.

00:59:51  
*Speaker 1:* It was a problem because, uh. And I have not checked up. I've read somewhere that Israel now, uh, said, yes, we did it. I need to document. I'm not sure I need to check it because for my next education. Uh, but I read that around November. They said they did, but I need to double check on. So don't quote me that one. But everyone apart from Israel and the US, the last time I checked, the Israel did it and what they did was they opened the gate saying, hey, now it's okay to attack, uh, physical, uh, supply chain attacks. And, uh, this machine can you can see this has not been tampered with, do not have explosives in it because someone wants to hit out a partner. I can't. And that goes for every piece of the of hardware you can give anyone, any company in the world or as a person. Can you guarantee that Apple have not put pumps? And can we guarantee that the. Yeah. Whoever took over Steve Jobs don't plan with them. They should say, hey all iPhones will destroy you. Pay me money. You know what can. And if I just showed that it's it's okay to do it. And that's a big problem because now the next attack will not be 911 with plans. Next attack will be, hey, can we affect something big? It'll be hard because it'll lead to the it'll be state sponsored level. But again, Israel managed to infect the entire production line. It was not something they did not get Ahold of a shipper of Peter's the when supply chain when they when the media. Peter's was in that level. And where to a lot of, uh, components. Article points come from electronic components come from they come from uh, for example, China, which do a lot of uh, it's a lot of components. And they, uh, they're I would say I'm not so worried about the auto insurance company because we can really affect those. But if we the motors that say, hey, Pete, need to put bumps in the hearing aids, that wouldn't work. But if China has had to put bump bumps in whatever that, uh, their factories are doing, they'll have to, because these government run putting could do the same for their produce. And he said, now it's okay to do it. And there will be more tests like that from both countries and from smaller, uh, terror groups. It will happen.

01:02:26  
*Speaker 2:* So how did it affect the situation in Denmark? So basically Danish hackers and like terrorists get the inspiration from them. Or is it more like on a standby?

01:02:41  
*Speaker 1:* It is not on what effect from us. Uh, because a single hacker can't do anything. It doesn't matter in that regard to physical damage like that. That's a nation state issue or a very, very big and organized group. Again, uh, Russia, with state help could probably do it. But right now we're blocking everything import from Russia, so don't care. China could do it. Some other country could do it. Single people cannot. So it doesn't matter much for us. For us it's more like limiting damage. For example, Chinese, uh, cameras with the backdoors. That's our report. We could expand saying, hey, Chinese cameras might have explosives. So it's about what? How about you? Do you trust Juventus? Uh, I would again say. And not paranoid, but, uh, to buy from Timo to buy the Germans from Timo. I don't, because who knows what's in it. And that could potentially, if I were to say, I just need to create havoc somewhere and destroy a trust for consumers worldwide. If someone were to sell a lot of, uh, potential damage devices on Timo, on Amazon and wish and whatever, and year later, that would be a massive blow to, uh, consumers. Well, one thing can be charged to the bank. That could be interesting. That would potentially be doable.

01:04:07  
*Speaker 2:* So what do you think the main threats are right now for Danish society?

01:04:15  
*Speaker 1:* That is a cyber attack from Russia.

01:04:19  
*Speaker 2:* Targeting exactly what? So what is the reason for them? Or like what is the main consequences that can be brought up.

01:04:28  
*Speaker 1:* My best guess is that if Russia wants to escalate, uh, let us say Trump is right at home doing whatever he's fucking doing. If we got to try to make peace or whatever is Putin paying him to do? If Putin gets his way and if the war don't stop, uh, and we keep supplying and he get more desperate, uh, the Russian troops will attack, uh, try to attack these power plants. They will try to take the Danish, uh, water. Uh, they'll try to take things infrastructure in general, uh, and we will get hit by that because no power, no hospitals, no water, no hospitals. Those are the main ones. I would not be as concerned about an attack on an organized attack on a hospital as such, because it'll be a lot more efficient. Because if you want to show the Danish people that you do not. If you help Ukraine, we we bother you, then hospital is not that interesting because he Amman hospital? No. Then should I care? Yeah, but if I don't have power for three days, I'll start to care. Those would be more interesting targets in public ethics and public opinion. Those are the ones I would go for if I were Putin. So that'll happen if, uh, Putin is allowed to get Ukraine. Uh, if for either you could give up or, uh, Trump managed to do whatever he's doing. Um, uh, we just had a report a few days ago saying, hey, in five years, if NATO do not if the US backs up to if NATO do not increase their military spending and Putin is allowed to say to build up and now he's been told, hey, if you take country, you'll have to keep it. You start again. And of course, again, he lost a lot of men. It takes time to fix population. But again, can you hear from China on North Korea? A lot of Spare manpower. Then it would start taking more countries. And if we try to go in and get help, the odds of us being patient is worse. I would also say that should again, the reason we have not been hit big is because Ukraine is a target. They don't need to go past Denmark, so they have no interest in doing much more than bother us or send a signal or threaten a little bit. We can find some things to open up the radar systems and say, hey, we are here just to know it, but they haven't done anything else. But if we were looking at a scenario where multiple countries worldwide were involved in the war against Russia, then uh, every Russian submarine, which have a lot of it need to pass through pass by Denmark. In that case, there would be sabotage. There would be threats. There would be, uh, damage, physical damage because Russia during World War Two, you could see submarines, but hard to detect them nowadays with, uh, measurements everywhere. If this war starts, then I would have to put sensors everywhere to see is anything coming. And Ross would have to do something to stop that. And that would escalate.

01:07:41  
*Speaker 2:* Interesting.

01:07:42  
*Speaker 1:* And again, that's for cyber warfare. But that would that's against Ross has to set a fleet if you're interested. There's a very good documentary about the Russian ship fleet on the air. It's a Danish satellite, but, uh, they're talking about, uh, data to people trying to track those ships. We have a lot of ships in the Baltic Sea that do not have a tracking channel. Is allowed to. Russia has a lot of ships that. But Russia owned by and by other countries. It was a ship a few weeks ago that there was two cables. That was a Russian crewed, but owned by a single protocol or something. They've lost secrets in other countries that are saying what they see without transponders that we cannot track without seeing them. What are these those ships doing while they're sitting here under these cables? What are they doing in the planting? Something we don't know. Other plans are pending sooner. Buoys. Other planting something to be used in a future attack or to disrupt or cause chaos. We have no clue. What? They're there. And not cyber attacks, but part of a hybrid war which would include cyber attacks. But if Russia needs to sail ships or submarines past Denmark, there would be escalation of the physical damage.

01:09:04  
*Speaker 2:* Are you knowledgeable about the website called Cloud CrowdStrike?

01:09:10  
*Speaker 1:* Oh yeah. Cross-site. Yeah, I know those those guys. Yeah. About the recent program.

01:09:18  
*Speaker 2:* Yeah. Would you would you advise using those materials in my bachelor thesis? Since I am not sure if the reliable source.

01:09:25  
*Speaker 1:* Cross-site trust CrowdStrike. Yeah, this arrived source. They are a security company. The, uh, to be trusted. Well it's good Palo Alto Unit 42 were some good analysis there. Also good. CrowdStrike lost a lot of credibility lately because they had a fog up where one of the updates to town all machines, they weren't and they took down a lot of airports worldwide and so on. Half a year or so ago, it was not good. I think it lost half the stock value of a week or so listed trying to rebuild, but I would not say don't use CrowdStrike is a good update. They just fucked up and they had a bad day.

01:10:09  
*Speaker 2:* So basically you mentioned the attack on the airport.

01:10:15  
*Speaker 1:* Yeah, there was an attack. It was a craft like the enterprise software and a lot of airport engineer software and the head software update that the ghost machine to blue screen. Every machine more or less. Uh.

01:10:34  
*Speaker 2:* So was it, uh, I believe it was last year when there were no flights.

01:10:41  
*Speaker 1:* Exactly. That was cropped. And the problem was that, um, for over a week, the only fix was to go in and delete some files manually for a machine. And, uh, let's say we have 3000 servers. Yeah. Two scripts to delete files, but they require windows to run. No, you need to open save mode, go in manually files times 3000. But for us if we get one can start CrowdStrike. And we are easy because we have, have uh, a few server rooms and we have virtual machines we can log into. But if you have a situation where you have a lot of physical servers spread over a large or an accessible area. Let's, for example, say we build women parks out in the US and we fly by helicopter or platform, stuff like that. Then you need you had to go physically out to every location to fix it. And those are essentially just window problems saying it's a supply chain attack, it's just the cost of themselves. But yeah, it's not so good. But it's not an attack. It was bad luck and a faulty update.

01:11:56  
*Speaker 2:* Interesting, interesting.

01:11:57  
*Speaker 1:* And I will need to leave in 15 minutes for my next meeting. I'm sorry.

01:12:01  
*Speaker 2:* Yeah. So basically, we can stop here.

01:12:05  
*Speaker 1:* Yeah, I would, I have a few. I have one more, a few notes. Let me just find them because I also read the thesis page and those few things I would do. I assume it's the first draft, right?

01:12:17  
*Speaker 2:* Yeah. It's just basically a draft. So it's not really a lot.

01:12:21  
*Speaker 1:* There was a lot of, uh, stuff I would rephrase if, uh, if, uh, it was not a draft, but the ones I had them, you sent them to send, you give me a chat because I had a second ago. One of them is, uh, not, uh, someone. It's precocious to the mean of Denmark. It's called the capital region. And I wouldn't do that because I had to do my own research. If you haven't recorded in translation error and you haven't with the malicious intent to build something else, I can't remember why it was just in the lower part of it. It's a rephrasing. Uh, and then, uh, about the CPR number instead of 2015, 2014. It is not it's an algorithm it created voted. Uh, in a party, I had to do some reading this link for these website on it, but basically it's an algorithm saying hey, this used something called Motus lv, which means that, uh, you for last numbers to do the check. Uh, there's only a limited number of correct, uh, uh, numbers using that. There are technically 10,000 or so, 5000 per gender. Around 250 of those would be accepted by the algorithm. So if you stop in the past and ask for CPR, you give a random number. They can check and say, hey, uh, that's not the CPR number, even access. So that can be you. Like the problem is that, uh, we did, which means that, um, when people started moving here, uh, from countries less Ukraine is a good example. We have a lot of people, uh, from Ukraine. They if they do not have their full, uh, documentation on, uh, A birth certificate, for example, or passport. That might be the situation for many refugees. When you bond and approve it. No. You can. In that case, people need to get a CPR number addressing you from that year. Okay, we're just setting birthdays as the first of ten year that year, which is great because we're birthrate. Problem is I'm just sharing my screen. Of course, that was that again with only around 250 CPR numbers per date. And you said every refugee to 1st of January that year you run out of numbers. Uh, and they've put, uh, these dates, they've put uh, uh, uh, Evelyn, as a, as the birth year, the date mentioned here. The problem is that if you run out of numbers on first in 1980 because a lot of data shows up, then the numbers, and then we start giving numbers without modulus 11, which means in that case you get a random number. But for TV spawn people they get model based, but refugees can't get a non model number, which means that you need to be able to handle it. In the old days you said, hey, that's not a correct number. Uh, error. You can't do that anymore. So it's only randomly if we put out numbers to those given dates. Otherwise it's algorithm based. So someone knew about C-band? I was complaining about that one. Uh, do you have anything else?

01:15:57  
*Speaker 2:* Uh, yeah. So basically, I will be not working in Chip since March, so my last day will be 31st of March. Yeah. So is it possible to contact you from my personal email, so I will.

01:16:13  
*Speaker 1:* Of course, of course. No problem. Are you getting a hide somewhere else or what's the plan?

01:16:20  
*Speaker 2:* Yeah.

01:16:22  
*Speaker 1:* Oh, wait. Can I ask where?

01:16:23  
*Speaker 2:* Yeah. Uh. Shark solutions.

01:16:27  
*Speaker 1:* Ah, shark. Uh, let me just see what I think it can be.

01:16:35  
*Speaker 2:* Um.

01:16:35  
*Speaker 1:* Oh, yeah. Yeah.

01:16:36  
*Speaker 2:* No, no, no. I don't. Okay. Nope. It's not those ones I thought about. Sorry. Yeah, I don't know that one. Uh, sustainable PvP products. Okay, perfect. Congratulations.

01:16:50  
*Speaker 1:* Thank you. Yeah.

01:16:52  
*Speaker 2:* But, yeah, you're welcome to contact. No problem.

01:16:54  
*Speaker 1:* Okay.

01:16:55  
*Speaker 2:* Yeah. Because, uh, I was I was really nervous about this aspect because, like, I'll be out of the system, basically. And if it will be a problem.

01:17:07  
*Speaker 1:* It's not. Again, it is a as long as you can. Of course not. And again, but we couldn't do that new report anyway because that's public. So no big deal. But yes, if you were were hired by the first place, contact us to see. Can we get help on that? Would say no, but it sent you into no problem.

01:17:28  
*Speaker 2:* Yeah. Perfect. Yep. I don't have any more questions. Nor.

01:17:36  
*Speaker 1:* Okay.

01:17:37  
*Speaker 2:* Yep.

01:17:39  
*Speaker 1:* Perfect. Then I would head down to my next meeting.

01:17:42  
*Speaker 2:* Yeah. Good luck with that.

01:17:45  
*Speaker 1:* Thank you.

01:17:46  
*Speaker 2:* Yeah. Thank you a lot for your help today. It was I was I was really, really impressed today by the fact, like how like political situations can affect even like Denmark because I was not quite sure.

01:18:03  
*Speaker 1:* And we small country. But the politics worldwide is a the problem?

01:18:09  
*Speaker 2:* I mean, of course, yeah, but political stance is very, I would say like reliable for Denmark and the whole world since, for example, like I'm also doing the research how the things are done in Ukraine and like how is it doing in Ukraine. And it's very, very, very affected even like deeply in Denmark, since we have like a lot of like dependencies right now on different countries.

01:18:33  
*Speaker 1:* Yeah.

01:18:34  
*Speaker 2:* Yeah. And you can see just as something as simple as saying, hey, Trump says here on Greenland, I might put in truth to get it in a normal situation, the response to someone say, hey, I might invade country. We would tell them to fuck off. But since it's our biggest trading partner and ally, we can't just tell them that we need to be diplomatic and say, what do we do? How do we handle this? And in normal state it wouldn't be a problem. But we haven't eaten in the white House, so that affects how we act. And let's change some rules. And and the whole world would have four interesting years to figure out how to this effect. Anything, and that kind of whatever he's doing can affect everything everyone is handling. Just to put out the World Health Organization during a flu, a bird flu epidemic in the US and saying, hey, my own healthcare system is not allowed to report on the casualties. That alone is enough to scare me and saying, hey, if these aren't pandemic and they're allowed to tell it, it could affect everyone. We called epidemic and then allowed to share information. Stuff like that. I think everyone, no matter what we do. But thank you and you're welcome to contact me.

01:19:48  
*Speaker 1:* Thank you so much. Yeah. Have a nice day.

01:19:50  
*Speaker 2:* No problem. You too. Thank you.

01:19:51  
*Speaker 1:* And good luck with the knee.

01:19:52  
*Speaker 2:* Oh, thank you so much. Yeah. See you then.