00:00:00  
*Speaker 1:* My name is Janos Nilsson and I've been in Houston since we made The reconnection. I started on this hospital in 2002, which means I have a long history of what's actually going on here. Uh, I have been had a lot of different responsibilities, and in 2009, they outsourced my responsibility and said I wasn't allowed to leave the building, basically. So I asked, what then? What can I get? And I got antivirus because no one cared, basically. And, uh, still no one cared. So with antivirus and everything else, uh, security wise, and basically seven years ago in the open, a place where me and my one coworker was not able to do anything but keep it alive, and it was security. There's no security department. There's nothing. Houston had no interest in security. The enterprise. That was it. Seven years ago, our leaders decided, hey, we have a problem in every department meeting. Me and my coworker told that don't worry about any SLA agreements on all cases because we know you can't handle them. We're working on it. Four years ago, we made a substitute department. Start with me. Like we told them and our boss. Today we're 26 people. Wow. We have not known any department in public service that increased that fast, but we have just as much to do still, because before it was enterprise. And now it's everything. And now we have time to actually go and figure out the problems. And every time we touch anything, a few skeletons pop out somewhere. Basically we have again, the problem for hospitals is we have literacy software and a lot of it we have we don't have any windows NT. We've closed the last windows 2000 last year. We have windows XP, Windows 7, everything else. Uh, the problem is it's physical. With medical devices. We can't just decide what to do because if there's 1 or 2 suppliers worldwide, we can put a lot of demands. But if they say jump or we have to do it because we the choices sometimes between what can we do? Can we actually, uh, do security or do we have to change security or saving patient lives? And let's just take an example. I'm not naming which department, but, uh, we have an issue where there is access to patient data. That's a GP issue. Everyone through the username can access it. That's a problem. Uh, we can only, uh, fix it one way. That's by closing the shares. It will close the shares, uh, around 120. Very, very important patient treatment will stop. The only other fix is to get new, new software that's already an EU tender, which takes up to a year and a half. Okay. Which means we cannot force it without cutting off treatment for 100 patients In that case, we have our, uh, information security write up. An exception, say, hey, we are now allowed. We know this, but we cannot do it. And this is why this is what don't mitigate it. And we're working on it, which means we will not get GDPR fines because again, you can't just write here, we don't care. Then you get a fine. But we can tell you why when you've made a decision, this is why we don't do it. And it's not. There's good reason it's not a problem. But you need to do the paperwork. And that's one of the places where we have matured a lot, actually, because before we just okay, people do it. But there's also a big problem because everyone just installed what they were they wanted, bought whatever they wanted. They didn't care about Cmmc it's easy to buy it and ask for forgiveness. And we've cut down quite a bit on that. Uh, people now learn that if they buy something that's illegal to use, it gets taken down. So we've improved quite a bit in that one. But there's still a long way to go. The problem is that we can't always win against medical software. We have a huge patient thing that don't run our antivirus because we end up on a micro level, and we lost that fight because there are two suppliers worldwide. They don't care that they bid on it. They don't, uh, they didn't care about our requirements for antivirus. And then after sitting up and we came say, why don't have enterprise or we can use your version and it's too important to do anything about. We can't win that one. We are doing what we can, but we will lose sometimes. But it's been a lot better. Uh, if you've been in public service, you probably know that. Okay. We'll do it tomorrow. That attitude, it's been normal for many years. Also in here. My new boss is hired to be a little angry dog who biting at people and getting tense and yanking until stuff happens. And it does that. He's very good at it. Which means that things work now. Took a year and a half for the organization to figure out that if me and my coworkers come and say something, it's actually important. And if you ignore it, it don't go away. You did earlier, now don't go away. And if they keep ignoring it, escalate to their boss. And that actually works. And even better, it is also taught some of our other bosses in infrastructure, especially that insecurity to peak demands, because then they also start to actually expect results and completely people are not doing it. So improved the company as a whole quite a bit. That works. Our problem is again legacy software and our users. The weakest link is always the user. And you know, in Houston, as you know, we are very open to what people allowed to do. Basically we have there will be a use case for almost everything. There'll always be an exception to whatever rules will to make. We blocked someone called. Uh, I can't remember where because I think, uh. No, no, we broke a huge supplier where everyone at the email can make a website because they used to make fake websites for phishing purposes. We block them because we had after 20 attacks from them, we didn't care anymore. We've allowed one user to access it because, uh, the Who department bought a small website on it, and it couldn't be accessed from here from the front page, which isn't a blog for her. So she's allowed to do no one else. There'll always be exceptions in this company. Uh, the other one usually is training, so to say, uh, pornography. In any other company, you plug it in our blog, it and we have a plastic surgeon can work. The psychological works can work. We have, uh, the psych ward. All the patients will basically need to be medicated or tied up. So we've opened a lot of stuff we would normally close any or anywhere else in Houston. The rules for people for employees is actually that as long as you don't install software on the computer and you don't break the law, we don't care if you do something that's wasting your time at work. It's between you and your boss, not between you and the IT department. We might be asked by your boss to give some logs about what you're doing. That's quite another thing. But we basically don't care what people do as long as you don't break the law. That is sometimes a problem from our department because we have just been saying he should they do that. And the question is, yes, of course they should, because why not? Do we care? We are not having any sort of test discussion saying what should people do? We've closed down three websites inside four websites the entire time I've been here. We've closed down TikTok and Snapchat because of cyber security. Recommend those because people tend to share, uh, GDPR validation and other stuff on it. We have closed, uh, just closed on the web because the team web basically want access to everything and on your phone. I know you've seen what they require, but, uh, if you install team, they basically allow you to take your phone off sleep mode and record what you're doing and send it out. That's in the requirement. We don't like that on our work phones. Uh, so block that one. And we during the Covid epidemic, we blocked one website. Uh, we had some of those main black guys who don't believe vaccines. They allowed to. We don't care. But they decided to buy a domain called fog mid-afternoon. We don't care if they make fun of our prime minister. Doesn't matter. But they put in a website where you can create a fake Covid 19 certification that we had the vaccine, and we can really allow open websites, we can create a fake vaccine information. So we bought that one. That is how we are. That ought to give a lot of security problems because again, people can do stuff. We are cutting down. We are being better at it. We are starting to look into other isolating machines. So if you download hack tool, if you compromised your machines, compromised it down to for some reason. In the old days, we will probably notice it at one point and a quarter and say, hey, what are you doing? And half our people do not have contact information on the bios, so we might try to call the Department of chase them down. It might take hours or days. Nowadays we work on access to on isolated machines. Say, hey, you done something we don't like? Your machine is now isolated then, which basically means you can't do anything. We can access it from our own solution and see what's going on. And we've tried to get some of that in so we can basically be proactive and stop stuff before we notice ourselves. Just our software scene should be enough. Okay. And let me just fine because. Oh, hello. Uh. Let's see. Just put the camera on. Two seconds. Uh, nope. Nope. Doesn't work. Sorry. Can you hear me? Um. Two seconds?

00:10:04  
*Speaker 2:* Yes, I can, but they have a very poor connection.

00:10:08  
*Speaker 1:* No problem. It's a we've talked before, so, you know, we've already started.

00:10:13  
*Speaker 2:* Yeah. Morning.

00:10:13  
*Speaker 1:* Vice mayor and my Teamsters question might not have heard that. Uh, we can say yes.

00:10:22  
*Speaker 2:* Yeah.

00:10:22  
*Speaker 1:* Yeah, we can still hear you. My teams might present a moment.

00:10:26  
*Speaker 2:* I'm. I'm dropping. Yeah. Okay.

00:10:28  
*Speaker 1:* But we're just going on here.

00:10:29  
*Speaker 2:* I'm standing on my side. I just want to. Yeah. You keep going, guys, because I'm going to write what I have to say.

00:10:41  
*Speaker 1:* No problem. You listen to recording everything, so if you need to go over it with her. No problem.

00:10:48  
*Speaker 2:* Great. Thanks.

00:10:49  
*Speaker 1:* Perfect. Um, a few tries to do our security presentation. You probably know what to get over here so you can see the screen.

00:10:59  
*Speaker 2:* Okay. There you go.

00:11:05  
*Speaker 1:* Basically. What? That one.

00:11:09  
*Speaker 2:* You have merch, actually. Sorry. You have merch?

00:11:13  
*Speaker 1:* Yeah, it's from our union. It's all I get for my money, but it's fine. Okay, but for some reason I do not. Two seconds. Seems just massively crazy to think.

00:11:36  
*Speaker 2:* There we go. The presentation after.

00:11:39  
*Speaker 1:* Uh, this presentation. Uh, I might have to cut a few pages, but. Yes. Oh, yeah. But there's nothing highly sensitive in it. Basically, this presentation is, uh. It's problem because if I start presentation just as work, if you're not in the docking station, all those Christmas lights instead. Very. Basically, this presentation is something I do for every, um, new person in my own department. That's why we started it. And then we had got information security, which is mainly lawyers. And, uh, what we called the other people, they are not technicians. So expanded to also teach them. Then we had local localities who are responsible for all software that are now run by CMT. They also wanted, and we have some other lawyers and random people to want to get this information. So we basically doing it on whoever wanted a run every two months or so. It also gets approved all the time. So, uh, it that might not be the same next time we do it. Oh, I do. Whatever. Let's do this. Uh, very. Basically, it's just about what cost. Doesn't matter for you. Actually, one thing might matter. Uh, I'll sit down. And two last parts. Uh, 95% of malware come through mails. That's a very high number. That's our main risk in who's done. The fun part is I started doing this in 1917. It's the same percent. Doesn't change. And even worse, one out of 13 connections lead to a malware side. That's also been the same since 17. I don't know if you go online is 113 hits on a malware side for you is not for me, and I hope it's not for you. I have no clue how the numbers are at high. Well, this is from firewall windows. I do check up on this data once in a while and this is newly expanded. You probably know some of it, but I'll go through it anyway. Um, but two things I really, really want to turn off this, uh. There we go. Just teach me. Uh, I don't know which country format you mind.

00:13:55  
*Speaker 2:* I'm from Ukraine.

00:13:56  
*Speaker 1:* Okay, then you won't mind what I'm saying in a moment. Because I had to get political in the last two months. Otherwise, I'm trying to keep this apolitical for various reasons. But the world changed massively after the Israeli, uh, major problem. I had to change this one, so I won't solve it anymore. But I'll try to install several countries, so. But basically, uh, before two months ago, I focused on the first one, the money. But basically, this is why I was getting attacked. It's my principle. It says money ideology comprised an ego. What happens? Money is the simple one. That is someone doing malware. We want cash. North Korea trying to get some cash for the perfect ideology. That'll be, a North Korea, Russia, whoever it was like, as usual nation states or organized groups. Compromised. There'll be insider threat. Someone's trying to steal our data. Some data for governance and data out whatever. Either on purpose or by accident. Both things happened. Those keys some years back where a guy who got fired from a Japanese probe because he went out drinking with his buddies and he brought a USB stick along with information of 4.2 million citizens, and he lost it unencrypted. That's not very good for your career. Not on purpose, but again, no good. In Denmark, we had a case some years ago where we, by accident, sent 4.5 million CPR numbers on a CD to the right building, which was another sort of status to think in that building was all the bed was delivered, which was the Chinese embassy. Not good. That's why I'm not considering CPI numbers to be confidential. More because we gave them all to China, basically. Then there's ego, the last one usually former employees. If you fire someone, if someone has some grudge on the company, somehow that happens. Usually for an employee it can be anyone. But those are the main reasons people take. As for money basically and not even like saying this. But if you see in Romania you can make around $8,000 a year doing software development, you can make when you're making big 100,000. Why the hell shouldn't you? If you do it in Denmark, you get cold. We have very, fairly good information security rules. We have. We have need, we know our banks and so on. And you can't bite the police. That's important part. But if you sit in a country, we can buy the police. Why the hell should I would do it? I wouldn't do it in Denmark. If I was in Ukraine, for example. I could probably get away with it. Uh, what? You can't do some of the basically the information, uh, cyber security network on the darknet is quite advanced. If you have around 2000 or $3000, you can buy a software to do malware, ransomware attacks, and the Email Institute. You'll also get 24/7 support. You will get a video support if you need it. You have. We have a three day. If you have a high case for CMT, we have three days SLA agreement service license agreement saying he will fix your problem if by access there they have a 24 hour level agreement saying then make a new version that won't be caught by antivirus. They have better support than we do. That's what you're up against. They're good and you don't need you don't need to know what you're doing. You can buy everything from them. And those are the small fees. Despite those are usually one will get caught. The ones doing software don't get caught. There was an exception a few years ago. Three of the big bosses got code. Uh, they were untouchable because they all need Eastern Europe and the sort of untouchable which they are because either in Russia especially, you do it for the government or the church, you or you by the police. But if you're stupid enough to go on vacation in the London room in New York, they know who you are in the courtroom, in the airport because you're on the plane as soon as you got on the plane. Hello? Uh, that's what they learned. But they're untouchable in Eastern Europe. Uh, sometimes you can, uh, try to tell people to stop doing it. One of our suppliers had a case where the hackers were in the system. They managed to track the guy, figure out who he was while he was in. Actually call this number and say, hey, we're looking with you right now. Do you mind stopping by the way we turned you into Interpol? He logged off really fast, but you still can't touch him. Of course, it's just perhaps a way out. But that's economy part state sponsored propaganda. Uh, how much do you read? Danish. Do you read?

00:18:18  
*Speaker 2:* Excellent.

00:18:19  
*Speaker 1:* Okay, perfect. We'll still do this in English. It doesn't matter to me, but if you want, this one is important. But basically, uh, just over a month ago, Social design agency, a Russian propaganda film, had almost all the internal documentation leaked. Russia for many years done propaganda, election manipulation and so on. No news there. But the usage denied. Just very hard. Denied when the company had in the last year had 20 meetings. Western government, their own commercial videos got called out and again they brag about, uh, election fraud. Uh, they tried to get attention for Deutschland in Germany, voted in and they got out and this election. So success. And in France, the same success the probably some of the reason why the rightwing movement is in the way because it's further Russians agenda to, uh, destabilize European governments, which is right wing. Just look at the US at the moment. Success. And one of the really fun ones was that they made a story about Ukraine, have some organs they collected, taken seriously by some media. So Marjorie Taylor Greene, one of Trump's big supporter us, shared the story. Yeah. Success. Because if you say 27 news believes it and they destabilize. And for example, in this case, uh, hood, the Queen was involved, but they got caught in this one. But it doesn't matter for them anyway. But it's just to show how to governments actually try to affect public opinion. Then there are states battle sabotage after the picture and walkie talkie explosions in Israel two months ago. Um, the bill from parties, what actually happened? Because at the moment, the only country in the world not saying this is Israel, but they got basically they called Israel's, uh, defense minister, called us a few moments about the explosion and said they were doing an operation in Lebanon. That's indicating that, uh, New York Times, which are fairly well known and respected news outlet, have told 12 now or present or earlier, what do you call it? The, uh, the spy who's confirming that is. Well, they just say it wasn't us. What I'm worried about is not that they did it. It's scary in itself. But the consequence now is that, hey, now you allow to put bombs and stuff, you can intercept. Can you guarantee that Apple know what happened to this MacBook before you got it? No you cannot. Can our supply guarantee if there's no explosive device. No they can't. And what do you do if now that, uh, spy agencies are not allowed to do actually as Israel did, create fake companies and produce the hardware themselves, what do you do? You can't do anything. And just to be fair, it's not just Israel. Um, Israel did also in 1972, where they put explosives in a phone for a PLO member. Um. That worked. But, uh, the US all did the same Cisco stuff. We used to use Cisco switches before. We still have some Cisco hardware. But the NSA actually had to intercept the hardware in transit, put the trackers and surveillance package on it, put the what? You call it the. There's a seal on every device that's saying, hey, if you break this, you break the warranty. Resealed it so it looked untempered and send it on to the customers. They did that for around ten years. It was Snowden leaked that one. Uh, and, uh, Israel and the US made a computer from years ago. Stuxnet, if you heard about that one. That's a fun one. The goal was to destroy Iran's centrifuge in the nuclear facilities to stop the nuclear weapons programs. It worked. They basically recalibrated the centrifuge, and they got physically destroyed. The problem with the worm is that is not a targeted attack. Just like the pages as well. It is not really targeted. So around 59% of the Stuxnet damage was in Iran. The rest is worldwide. And just to show you, the implications are central in particular. And they ought to use interviews. And the same brand as Stuxnet also have been hit. And that is a problem because spiders are now doing attacks that might hit someone else. Because honestly, if this well had. Done something with that hit 2000 people and they knew who they were doing, it would probably be called legitimate. Yes. It's not good, but it's legitimate by warfare. But when it hits 3500 wounded and only a small percentage of the length of the target is no good, but that is the world now. And all of this was new last time I did it, because I tried to keep it open until now. Now I need to okay where it's coming from again. Emails. Uh, this is an example. From where? In Houston. Hey mailbox, meet Susan Size and click on this link to get it fixed. And I use this base to do like this normally. Um, my favorite extra one of our dean's newspapers they have for banner advertisements. I don't need to take it, but I need to have the banner, uh, publisher, because they need all their customers. And, uh, as I mentioned earlier before, porn is my first example. When I started this, uh, back in 2002, uh, porn sites were dangerous. Uh, basically in this, uh, every month, we had to deal with our, uh, portals. I think they called that in English. The one who taking patients around the hospital and so on. Uh, because they are men in the 50s, on 2472 and aboard. They watch porn. Half the porn had poppers. You clicked on us. Broke the PC we installed every month. An agreement saying this one is for the heart. Stop! And you will not use that porn. The rest break as a one. We fixed once a month. All. When you call that happen for those and the night shift on the psych ward nowadays porn sites. Cell porn. That's by the lithium. I'm not afraid of Pornhub. They have a lot of extra because Pornhub, they have millions to do the security. That's the business extra. They don't have the cash for it. I'm worried about the extra bit. I'm worried about public government sites because there's no country in the world, Western world, that haven't had at least one government or news site hacked the last year. Not. It's only going to get worse. I'm worried about something I should trust, uh, to know. Sparta. There you go. Yeah, yeah, they will look that one. Yeah, yeah. Uh, some years ago, one of my suppliers called and It's a genius. You have to shut down spots right now. Why? Because they got hacked. They put a severe attack on the 10 million button. So anyone who clicked that and I can't remember the flash. One of those two. But you didn't have patches that day. You could. You could wonder why we should shut down. Access this button for 14 days until the IT boss on in writing guaranteed to clean. And those are trustworthy sites. I will not blame. I'll blame a nurse for clicking on this one. I will not blame a nurse for clicking that because that site puts the trust. That's my focus. Trust resides in the USB devices. What happens if you drop some USB sticks down in the parking lot? This is from a US survey that dropped almost 345 of them actually got activated. And we have seen attacks in Denmark, people dropping USB sticks in the parking lot of a few companies and it'll work if I drop 20 USB sticks, right? Uh. Uh, what did you say for handling on them payment negotiations? I guarantee you 50% chance. It's not that hard. Sadly. Then you have a little free software. I said we have a lot of latency, uh, to no integration in office documents. So if you are doing something word and you link the word file to Excel, you can transfer documents between those. You know, for example, making the word document that link to an Excel file. So would update the info in the word document if the Excel file is changed. Okay. Simple integration. Uh, before that was something called DDE. It's not been used since around 2000. Some Russian guys found out two years ago. Hey, it's still working perfect. And, uh, we noticed because someone has got Russian letters and they're stupid enough to open them. Fair enough. They're not stupid enough to click two times on word document version text. Luckily, because after two clicks you had full access to the time machine. Basically, I made my own version just to check with my boss. Took some information from our website about security and would hey, this has been approved by Operational Security. Just click yes on the pop ups. If you did that, uh, all you can see was this one, uh, sorry, one undisputed exception formula. And, uh, that one, if you clicked on it included this one down here saying, hey, we are now running CMD, which means you can run a program. I started to explore, I started this website and started a webcam from a cow, uh, building in, uh, somewhere in Jutland. But, uh, it's just a proof concept saying, hey, I have control of this machine. Now take two clicks. Microsoft didn't want to fix it because this work is attempted. 14 days later, they changed their mind. But it took a little while. Then you have a Bitcoin mining. It's not so popular anymore, but in pirate Bay you know that one. They did something completely legal. Let's say, hey, when you use our site, we use your CPU for Bitcoin mining. So 100% usage while you're on the website that's legal. If you make your own upfront, you could cook, you make your own website recipes. You don't want people to pay for the use or use benefits. But you say, hey, I'm using you resource Bitcoin mining. That's legal. If you take LA times and put it in for three days, it's not legal anymore. But that's a similar take. Then you can use them to affect cell phones. In this case they put in a it had access to everything. And the interesting part for me is that the security guys, they actually did a small check letting run run on 100% CPU power for two days. They barely got guys removed the battery casing. That's the casing. There's physical damage. You can physically damage a phone. It's not that fun. Um, that's what happens. And the reason it happens usually is because people don't patch in time. That's probably a focus for you and for us. I can see that right away. Uh, patching is the most important thing you do, not the security. We'll go over some of our plans for patching after, because you need to know that for what we're doing. But, uh, this one is a very good example. Uh, do you know about the mask incident? Yeah. Yeah. Perfect. Uh, this is what happened. Now I'm just going to get up to it. So I used to stand up doing this, basically. Back in 2013, NSA, American spy company. Uh, they had backdoor to windows. It got stolen. That happens a lot of spy companies like backdoor because he then can actually fix something. Back in 2016, a group called Shadow Brokers started They had the tools. They put on an auction for in 2017. In January, Microsoft figured out there's a problem. Microsoft has something called Pets Tuesday. It was second Tuesday in the month. They do a patch of everything. The only patch on Patch Tuesday ever for the first time ever, the drop pack patch Tuesday and did emergency patch that's never been done before. Is that important? That was in February. In February also saw the first revised total request on that one and superstar to do uh uh and protection against it. In March Microsoft made a is B update for supported wizards. This is how you do shares on windows. That's how it spread in May. Uh the first one cloud big begin. There was no mask that was uh National Health Service in the UK. You know about that one. If you don't, don't worry, I'll tell you. Uh, I'll do that one. It's easy for me for stand up. Sorry, but, uh, Basically um, in on May 13th, the one started in May 13th. Uh, they made an S&P update for pen 2003. Those were the support Microsoft never updated support before that day, the first time they ever did that. Is that important. They were not legally in any way required to do it. They did it anyway. Uh, this one took down 60% of the UK health care system 14 days. I've seen pictures of people from the National Guard in the UK helping reinstall PCs, because they didn't have enough manpower to fix it. That is very, very expensive. That helped. We started people start noticing at that point in July and we got hit by an invasion of this one because they still haven't put pets in from Libya and we hadn't either. To be fair, we also patched that weekend and the weekend with it. Both weekends. We didn't have a security partner at that time. That was me. Uh, I noticed that before my boss called. I actually read up on it, but, um, we ordered pets all the service this weekend. Normally, if we patch basically in Houston, we have over 3000 windows servers. We have very little. It's been a lot better. I would say 10% of sales. We don't know what's doing. It was 90% of the time. I can't restart a server without knowing if I killed someone to do it. It might be an intensive care server that we again, don't matter. We patch sane when the mask attack, we patch and people can complain after to our bosses because not going to change. We had to do it, but it took down a lot. Then as we build 20, this one is fun because this is not not solved and there will be some security researchers think it found 20 security holes in, uh, the TCP IP. Do you know what that is? It's how you do instant communications. In a version from 1989 and only a version that did the paperwork tracking say, hey, who bought license to use that version? And the following companies, they're following this list who we don't use and who's done half of them. We don't know what we have from them. They don't know the hit we had to inform. Uh, was it the to do? Yeah. They were not one of the other companies on the mailing list. We had to inform the teams about the hit because they didn't even know. Although it is public knowledge. It's still not fixed. We can check for it. We can check and check for it. But as a private person, you have no clue. This is the people where they say we might be here. We don't know how much. I'm not sure about you, but I really don't like that. Uh, I think we have them quality time with GPS communication and NASA and Lockheed Martin does airplanes. I don't like that anyone would potentially be able to run something on their thing, on their, uh, unit, and they don't know what's affected, and they still don't. The really fun part is it's not fixed. And potentially because the people treaty is from who officially polled and could be tracked. Potentially. No one cares. Not big deal. Uh, people aren't. For example, they use it in one version of the media center, nothing else. Hey, we don't care. But potentially every IoT device in the world is hit. That worst case scenario. Probably not that bad, but no one knows and no one cares. That's fun. So whenever you buy a kit at home, just think about this one saying, hey, someone might be able to encode on it because I have no clue how to protect it. I can protect myself. Span, Mills. Again, we talk about 94% of attacks in spam meals. This is the normal. This is one we got hit by the. This is from my coworker, but it was from the user themselves. So, hey, I send myself a mail with the text file. What? What happens? Click 19. People did that in a week. That happens. One of them, I only had her word for it. I didn't have in writing. If I had, I would actually control. But but I quote again, we are not evil. We don't punish people who make a mistake. It happens. So I called with some like head and I called user talk to them, say, hey, you need to be more careful. If you get a media to understand the code, our services will help. No problem. Reply was no, that's not my ability. I am not a. I just have to pick up everything. I'm not paid to actually think basic. Um. She's dangerous. She should be fired. But I only had a word in a phone spoon for which I couldn't do anything but my jeep. What did I get? Two of them, to be fair, had actually thought. One of them thought, hey, this is probably from a printer. Someone printed something on me. Fair enough. You just want what you thought. And one of them was for a shared mailbox. Again, fan of not good. Then you have what happens when people fuck up, but it's actually not tuned on purpose. The one library in Denmark sent this mail to some of our users. And of two. Basically we according to EU account, but if you send it to use it, you can contact us and send a scan of your Danish health insurance card, passport, driving licence to Amazon. That's illegal. You're not allowed to ask for any of this. You send an English to people who don't know they have a deal with you, and you're asking for legal information to send unencrypted to an encrypted email. That's four different breaks. I had to call him and ask him to. One of my co-workers had just been hired there so I could call him and say, hey, what are you doing? But that's not in bad faith. They just didn't think. It also happens. We have to protect from that. For example, we have a Saudi Arabian health insurance company. They cover all the embassies in the coming area from not just sorry, but all of the Middle East, basically. They don't care about GDPR violations. They send emails, all the patient information unencrypted. I've seen that a few times. And I actually said, hey, I'm heartbroken because this is this is not good. And I called the department saying he just to be 100% sure, shouldn't I block? No you shouldn't. We know they're doing this. They don't care if we talk to them. They still don't care. We remove all patient information when we reply. So we don't break the law. But they don't care. We can't do anything because we can't be responsible people sent to us. It's the same if you as a private person, email your doctor with the CPI number in the journal. That's legal. It will apply to you in that one. We're breaking the law. That's all the problems. Sometimes we have to take it over and say we have to. If we apply, we have to do it in a box or we have to send a physical letter. We can't do it on mail. And again, the standard phishing, basically we are not respond to everyone's phishing attempts. If you mail from Nigerian prince we don't care. You get one single who's that transmitted. We will care and block it. This one led to this attack. He used the access. Put it in. That happens. This one we don't really care about. It doesn't matter. Oh, this one is fun, actually. You ever seen that one is a porn blackmail thing? He will record you. And what you watched when we recorded you. We sent all your friends and family. That's normal. That's common. We get them all the time. The fun part of that one is, how do you make this more legitimate to get people scared? And I can see something fun. Um, and I hope you know this website. If not, you will use it when you get home. Uh, hopefully you should. Have been owned. Do you know that one? You will need to learn that one. This is a website by an American security researcher. It basically say your email. Is that in any breaches is unknown breach. So if the company you signed up for get hacked, he will inform you, hey, you probably need to change your password if you are smart, which you of course you are. You do not reuse your passwords, correct? Yeah, of course, if you reuse passwords, if you got hit one time, they have everything. Um, in this case, I usually present myself because I know I do anything embarrassing in here. I do not use other people when I'm teaching because they might suddenly start dating site or something. Not good. But Over the last 103 million accounts in 2013, Nixon lost something. LinkedIn lost 164 million. And this is a fun one. LinkedIn back in 2012 lost 164 million. Email address and password. They did what they're supposed to email. They're using the heat. We had a breach. Change your password. Shit happens. Four years later, this dataset got sold. And when that happened, someone figured chickens. There you go. How do we make our porn scams more reliable? Hey, we buy the LinkedIn because we have emails, which we'll be anyway. And to prove we've heard you, here's your password. If you use a password, you know you get more scared because they now have some personal information. It might not be that password anymore, but it seems more legitimate. We had nine cases in a week in Houston, and then we actually this website, you can sign up for it for companies also. We do that and we email for non-users saying, hey, you will get these emails. Don't don't panic, you will get them. But it happens. And uh, that's basically one thing I say everyone should sign up on that side saying, hey, is there any risk I could get hit? Notify me. Do that one. Use your own email. You will get emails. You will most likely be on this list for something. I've seen people learn, but it is rare. Actually, just one more thing and the reason why I don't just show everyone. Because there was a list which peaches is loaded in there. You can't buy the information from him. You can say, what's the password? The security researcher working with the FBI on this one, but you can use it to protect yourself. The problem is, again, any company get hacked, no one is safe, and it's not their fault most of the time. Sometimes irresponsible, but it's not always their fault. LinkedIn probably have good security, but shit happens. Problems. The consequences when it happens. And that's when you get bad. Because, uh, where do you have it? Adultfriendfinder. You know that one adult dating site lost 4 million. Date of birth. Email address. Gender. Location. IP address. Race. Relationship status. Sexual orientation. Can I use that for anything? Oh, yes, I can of course blame and say, hey, do your wife know this? Perfect. Two pay off. Of course you do. Even worse. Let's see. Where do we have it? Is the medicine heard of that one? If you've got Netflix that promised a documentary about this one. Okay, this was an adult website with a very charming An idea. They had an advertisement on the station some years ago. I bought you a marriage. Get an affair, which I'm basically doomed. Extramarital affairs. They lost everything. Uh, three. 13 million accounts. Date of birth. Images. Ethnicity. Gender. Names, password. Payment options. Phone number, physical address. So, yeah, you can ignore my emails, but I can physically email you. Prove to your wife the effect. Uh, lost everything. As an extra bonus, they lost everything, including all the source code. And it turned out that almost every female on those bots trying to get our stupid, stupid men to fall for this one. So actually, no females on it. People commit suicide. Or this one. It has implications of what we rolled out because some people didn't like that one. Uh, some of the users so can actually have consequences. And my personal favorite, because again, if I bust, I'm happy to say I'm a bastard. If I would attack anyone, who would? I'd say, would I take the one from baby names? No, I would not. I would attack it often. Find it because they're more likely to pay if I will pass it. I go for this one. Um. Bom bom bom bom bom. Why do we have it down here? There we go. Is there a sex taboo? Because I might be able to explain to my wife why I was signed up on a site for extramarital affairs. I'm not able to explain why I want sex with the dog. It's only 3002 and four people, but they're kind of happy because you don't want your co-workers to get an email about that one. And that's a consequence of activism for any website anywhere. And some of my job sometimes is to try to tell our people that get hit by something like this, to try to help them how to handle this or don't be afraid about the porn scam. It is not dangerous. interest. It is you are not here. It is only an attempt to scale, to pay up. For those grants like this one example where it tasted bad. Normally I would since I've been allowed to use the information here. Of course, the one of our middle managers, the Mid, who said be this nuisance does seem to become so reliable. Email email his direct uh support his most high employee. There's no not a single grammar error on this one. Uh, they know some of our problems. Always need them. He just log in to this internet site. The only mistake was the wrong company logo. He didn't fall for it, but he's in charge. And that's what I'm afraid of nowadays. God, you seem the easy scams where the misspelling everything. That is not because they can do better. That's because they weed out the, uh. They don't read out the fact that you did. Because if you, as a scammer spend two hours emailing 4 or 5 times with you and then you get suspicious, you waste four hours. If the people who fall for this, you make it stupid enough. The people that are the one who's got to go through all the way. That's why they do it and they make money on it. Sadly, it is money. But they can also do this. And nowadays, with the ChatGPT and so on, you can also talk things in real time. So of course it's easy. If you want to scam people then that's your fault. If I had one of those. The very basic thing he omnibus. I need to send some money. It happens all the time. And in our case, the problem is that we are very open in Denmark. Uh. I would say that half the employees in Houston have the emails on our website. He is the department leader. All of Chiba. Someone. Hey, if I want to attack someone, I claim to be the boss. I Tag. Who's the secretary or in charge of finances? Same goes for the the the union. They have a lot of, uh, file details about, uh, their, their expertise. And they will, of course, as you have to Denmark by law or to have, uh, pursued. Um, and. Hey, Foreman, let's I need of course, I'm going to see them and and let's see who is in charge here, who's in charge of money? They did. And of course, the mediator and claim. That's easy. Usually we will get them. I can Google the two names and then I'll find it pasted together. And they do that and it works. In this specific case here we had a transfer from €9,500. And what they do is basically they keep uh, if you apply, they'll just keep, uh, as he's done yet. It's done yet so people will forget the normal way of thought and just do it for the boss. And nowadays, the smarter because the bank transfer can be taken back. You can call your bank and say, hey, that's a mistake, call it back if there's still time, which means that you do not do that anymore nowadays. You instead ask for iTunes gift cards because once they send, in this case, the private have a meeting and need help getting a common iTunes gift card online. Can you fix that? For me, it's very bad grammar and is of course completely stupid. Uh, the trend for 2000 2500 gift cards in that one. In the last two years I've known two cases where in Houston they sent a gift card. That's the one we know about, but say, hey, we eat it. We don't report to you. I don't know the ones who didn't report, but at least two people forward said. And 2500. That's a good paycheck if you're living in Ukraine, for example. I don't know what's the yearly income in Ukraine before the war.

00:48:38  
*Speaker 2:* I know the monthly average income is around 1 to 2000 Danish crowns.

00:48:44  
*Speaker 1:* Yeah. So it was a month payment for that one. Perfect. Just need to tell people that your yearly income is done and it works and people fall for it. Sadly, we try to actually I try to say when people get caught in this one or get in, just get it and fit, I will use. I'm not just close to keys, I'll just call them, use five minutes explaining this is what happens and nowadays if you want, if you ask for money, you need to meet him physically, not email or phone physically and get it approved. And we'll get to that in a moment because they'd get worse. The consequence stays the same. One of the big museums, they lost over 800,000 and a half a year because they used to ask big amounts about art and to have a year to notice It happens, then there's a lot of scams, if you've seen that in the news lately. Um. That's expensive. In 1922, there were a change in Denmark, a loan to get 40.5 million. The voters got 21.9 million out of this. There's people again committed suicide with this one. It happens. Uh, old people who lost their life savings suddenly to whoever said they're nice. And the fun part? I don't have had you yet, but I'm a man, which means I will at least once a month, get some nice woman in a swimsuit. Who wants to talk to my credit card on Facebook? That's probably normal. Are you on Facebook?

00:50:12  
*Speaker 2:* I have an account, but I don't use it. Yeah.

00:50:14  
*Speaker 1:* Yeah. My guess is you'll probably get invited around once a month, usually for people in military uniform or in suits who would love to meet you. I'll say, I guess on that one. Uh, is your Facebook registered in Ukraine or Denmark? Because that actually matters.

00:50:28  
*Speaker 2:* I think, in Denmark.

00:50:30  
*Speaker 1:* Yeah. The reason is my wife is from the Philippines. She's never had an attempted scam because the Philippines are poor. There's no money in trying to scam them. The soon the moment she moved to Denmark and I was to get the money. I was surprised in that one myself because I thought the worldwide event is not. They know where is the money. There's no profit in scamming poor people. I find it actually interesting. That's why I'm using an indication because it happens. The good part is that in 2023, we're down to 17 million in Denmark. But it's still a lot of money and a lot of people's life savings. And there have been a lot of news stories the last year about it, but people still fall for it. And there's deep fakes. Those are really fun. Uh, Taylor Swift recently had the pleasure of, uh, have deepfakes of her and our football team in pornographic regions. That's not that fun. They actually got an in Congress in the US. Um, but what can you do? Not much. You can make it legal. It already is. There's a test in 2019. I haven't found any new tests, but the Detroit Security Company found out that 96% of online deepfake videos was non-consensual pornography. So, hey, your ex, you whoever you want to stalk, whatever you want to do, someone famous you want to see in porn situations, that happens. It's normal. And so then you female you are more attacking I am people don't want to see me naked. They want to see a unit that is set to the keys and they use it. And obviously I'm most scared. The stock situation that we got, and we have other cases in the region where people have been stalked and we are trying to help. What are cases where people think they've been stalked and are not? And that's the really not so fun ones. That's the one I usually handle. I'm good with people because some of my co-workers are black and white and will say, hey, you need to pixel together. Stop this. You are you insane? I don't say that. I'm trying to help them. The problem is, we cannot, as IT departments say. You need psychiatric help. We can talk to the bosses. And in one case, the boss has helped and noticed the problem. And he actually got help and got better. He was heavy. In another case, she could fire because she couldn't do a job. That's probably on your side of it. Is supportive of Morrissey, but in other case, he got fired because she was spending five hours a day being paranoid and being hurt. And it happens, sadly, with so many people have here, we will have people in all situations of life. And then there are the really fun. That's where it gets scary, because deepfakes could be used to scam and ER in the UK, completely lost £25 million in February on that one. The people smart because it wouldn't work in Denmark. To be fair, I don't care whether one text is more from me, but what they did was saying, hey, in Asia the culture is that if you are not the boss, you shut up and listen and only talk. When you told in Denmark you wouldn't do that. If my boss during a meeting tell me to transfer some money, I would ask what the fuck is doing the issue? Don't you do what you're told. So they set up a fake board meeting filmed like this from here on board meeting board, which is here. And the British chief economic officer at the end, which mean not a close up, but enough to be convincing. Then they made an entire one hour board meeting fake all of it. And the in the shots that he presented yourself, you have 30s the guy talked for 30s about who he was. He was in the board meeting and during the meeting he got orders to transfer around six times in total, transfer $24 million around. And he did it because that's what you do in Asia. It worked perfect, Which means that when you get a direct call from me, you're asking me to transfer money to those? Nothing. No you don't. You have to meet him physically now. Because we at the moment you can do real life deepfake combined with the AI like chat GPT three, which can speak Danish. So when you reply, it can do it and.

00:54:45  
*Speaker 2:* It's.

00:54:46  
*Speaker 1:* Hooked up to deepfake software. It will be able to do video replies and do conversation. It has been done and is not only going to get worse. That's what I'm afraid of, because I cannot afford a nurse for getting a call from her. Video call from her boss as transfer money. I can folder for the fake email. What happens? And then there's misuse of law. I don't know if you're covering that, but that's also a big problem because you can abuse the law in many ways. These are two recent cases. This world heard about that one. It's a bad one. Uh, a couple went to Disneyland, us, and eat a restaurant. The peanut allergy. The informed, the restaurant. They fucked up and gave her a lot of peanuts. And she died. Shit happens. The guy sued for $50,000, which is no offense. Nothing in the U.S. got a lawsuit system. And for first of all, it's a restaurant in Disney World owned not by Disney, but by whoever read the place. They should, of course, said he is not us. Sue these guys, they rent the restaurant. These things did decide to say hey, no, because you signed up for this. Plus, when you do that, our Tom service said you are now waiving your right to do a lawsuit on Disney on any reason, including we've done poisoning. Uh, Disney got smart and decided to pull that one because it doesn't seem, uh, Uber is not so nice because a couple in Uber that render it like Uber, they got damages both from the hospital. Massive damages should happen. happens. The lawsuit and the right, the law. The lawyers actually managed to convince the judge that because the last update added, the weight is the right to trial by jury in case of an accident. So no. So you can sue. So if you sign up for Uber Eats, uh, don't use an Uber cab. Or since it's ordering the Uber Eats service, don't use an Uber because if there's an accident, you can sue. And that's a problem because not one person will not see that. And in our case, we're gonna, Houston, have our lowest rate, our old contracts. Enough to see they're not some stupid little detail like this somewhere is the. Hey, in case the system breaks, we're not responsible. On page 215. I don't know, I hope I'll always do. We had one case some years ago in hospital. No one died locally, but we had a company and not naming names so you can use it. Probably not usable, but just to explain the problem. Um, the, uh, was an intensive care surveillance unit, which means there are nine computers, one for each intensive care bed and a computer with a result of all nine bits at the 24 over seven staff. Uh, pleased with that. Uh, surveillance loses internet access. What do you think happens? It says heart failure. All bets on an intensive care unit. That's not really good. Luckily, the bits did not say heart failure, but otherwise people were going around the ship saying, hey, wake up. But that could have actually, worst case, kill people. Uh, the couple's reply was, ah, we don't care. Supposed to do like that. Um, the guy who said that one of the two employees in the country, we told him politely that he was not allowed to go near a hospital for the next half year. He could can send school work if you want to talk to us for that one. But that is our company. Our suppliers can do that. Then again, there's a hacking from the foreign forces, in this case Russia. They hack the defense for two years, some years back. Russia of course. Do not hack because the Russian state did not engage in computer hacking. Completely true. They have. They have the groups for the high. The state is not doing it. It just has groups doing it. He's not lying. And the real fun part. How did Russia get in? Because Russia is good. Russia is very, very good computer. They have very good people. So how do we in all the manage to get the login information for an unclassified web based mail system. So yes, we send an email. Put in your code. That's a Danish defense for two years because someone phishing made it a National Health Service announcement for English security. Uh, In these hospitals, 60% of the UK hospitals were down 40 days. We'll find that was. What did that cost? £180,000 was the official number. I don't know about you. Do you think there's some little, though? For 60% of the hospital in 14 days. Good, because we also thought a little, though. Uh, last year, the Kingdom better estimate £92 million. I'd really love to get hold of the guy who gave that number and show him that number five, because that was something. The person should be fired. It's probably the chosen, but still not good. It's probably higher than this. But this this one. Get mask got hit. They caused a 2 billion official. That's the official number. Yeah. The real fun part is to know why they got hit. They were not the target. This is an accident. This. And I'm not judging. Which means that some group who speak Russian. I'm not saying Russia because they don't do that, of course, but they speak Russian. They don't like Ukraine. So let's start with Ukraine and Ukraine. You have a interesting rule that says if you need to do a business of the government, you need to use the specific economic program. And the Russians hacked that one and put a backdoor in the last version, which every company in Russia, in Ukraine needs, including match department and ask have we been? So they connect to everyone worldwide. So the matter why did that and took them down totally. Basically what happened was metal and even machine. They had no clue where any container or what well what was or what wasn't then? Nothing. The only reason mask exists. The company is pure luck. They had one Active Directory server in South Africa that was down for maintenance. If that has not been offline at the moment, we've closed the people with regard to done fetching the server physically. There are 2 billion. On the upside, the survived. And this is what got the cyber security focused in Denmark. We in here could feel a very, very high increase in people calling our servers and say, hey, that mail I got, should I click it? This helped us basically every time I meet a mask employee who was there at the time of thinking because they took one for the team. We were very happy about it. And who is that? Again, 94% of it takes us from email. We get 6.8 million meals a month and let's see, 4.5 million clean, 1.9 million spam, 3000 files. That's what we get. And sometimes emails get through and people click on them and people don't think again, we're big. We will get a lot of meat. I know, Patty, I get 200 meals. It happens. This physical security, you ask when you got the cart down there. Because people do not think this is my co-workers just to say, oh, I need to get in, okay? Because I heard the door. If I don't know the person I need to check up called the get in. Somebody get pissed. You're not allowed to say see that as well? Yes, I am, and you should too, because we always participate. We live in. There have been cases where we had a guy who just walked in the door, uh, go up on third floor here, go into our boss office, which means this room and that room, look at these two rooms and steal a phone from the service desk. We have a video, but he couldn't do anything. He tried to get come back a month later. We recognized him and threw him out and tried to get up again with him out again? We haven't seen him since, but that's how it goes. So physical groups, it's important. And for this card, when you get hired here, uh, you get a post on the backside of a card with your Pin code. Um, for the first time ever, last time I hit this education. Because as people can see card. Yes. Can see the backside of your card for the first time ever. Even had to remove a piece of paper the first time. But I would say 20% of building at least will have their Pin code on the back of the card, so drop the card. I have access in their name.

01:03:31  
*Speaker 2:* Truly, what do you think of.

01:03:34  
*Speaker 1:* Uh, you won't have on this one? You probably won't on on this card, but. It's not like that. It's on a post-it note on the backside. But you won't be on the bed only here in the building, because you need to get through our darkness.

01:03:53  
*Speaker 2:* Oh.

01:03:54  
*Speaker 1:* The problem is that we cannot block who came to hospital, because most places in hospital you need access and patients will also have access. You can't close off the this the intensive care unit or the emergency unit just because it's secure. I would love to, but we can't. The problem is with cards that you can get fines. People abuse it or you fuck up. Uh, Midland, uh, got a 202, a $400,000 fine. And the police, uh, investigation, uh, for breach of security and cash a few years ago. You know how you manage to get that high? It's very simple. Um. On, uh, every employee and patient. That is why they got the police report in Houston. One stop. Got access to a building with around 100,000 fiscal patient journals with the journals and, uh, personal information and user numbers, and everyone got access with keycard. They get access to everything on the buildings, no matter who they were, including patients. That's suicide. As a penal code. Uh, this is a fun one. This from a leak of a 3.4 million pin code from a place we can choose to resolve this top ten. If you try those ten on anything that is four digits, you have 24, almost 24% chance of getting in things a bit a bit high, but that is certainly the case. Especially a problem when you have stuff secured with a padlock with pin field. This is a command. It's a company that are using and are doing a destruction of sensitive material. You have the release. Also, we have them here. Um, I fucked up a while back here to print some documents for my wife education. She's a nurse now, and I need to print some stuff for her. And the first thing I did was third paper. About what? To print down this box. So how do I get into this box? How long do you think it took me to get to this box?

01:06:04  
*Speaker 2:* Good A day.

01:06:05  
*Speaker 1:* 10s.

01:06:06  
*Speaker 2:* Oh.

01:06:07  
*Speaker 1:* And our Mondays. Uh, basically, they had a the code was set to one, one, two, three. It didn't take a rocket science to say he should probably zero, one, two, three. And then because I'm again a bastard, I said, hey, how about the other, uh, bins on the, on the building? And they all used the same code, so I had access to our entire direction. And it contains material perfect. A tool set of who was the who responsible for our contract on Mondays. They didn't care at all. No, three times nothing happened. I told our lawyers who told signed off, and then they changed code. To be fair, it's not top ten now. I tested, but they changed the code. Well, it's really scary for me as a private person. Is that my wife's from the Philippines, and which means you have to renew your, uh, permits to stay in Denmark once in a while. And I got to, uh. the willingness to listen and the trouble whenever there. So we had to wait just at the. When we were being processed. And I asked, by the way, that bin over there, do you know the code? No, of course not. Try this one. They use the same code. All their fucking customers. Which means I just need to buy a college jumpsuit and look like a janitor or something and say, I need to come in to the bins, and I have to be able to steal papers. Perfect. And whoever is the service, which is probably half the Danish government. So I could try and see what happens there. It's worth a try. And people don't think about security, sadly. And this one again fits. This is from I take my new. When we high new people are taken to hospital to show them what's actually happening in the hospital because the IT world they need to know what's hospital, how does it work? You know, if we tell the the sellers and how you walk around the turns on the hospital. And this is in Russian, of course, you can try to hack through our firewalls, but if someone living in Denmark might place a small device there, they are there because they have access. There's no surveillance. You want to walk in if they want to steal something. Uh, this is a, um, the delivery area, the device. There's no one else, so I have no clue what's in these boxes. Might be interesting. I figured the boxes were locked. Is probably interesting. And there's a four digit code, too on this one. Perfect. Four digits.

01:08:36  
*Speaker 2:* Let's see.

01:08:36  
*Speaker 1:* Could it be one of these four? I'm not sure. I didn't test, but with a try, there's no way to stop me because no one knows what this is for me. Just to say it happens everywhere. Uh, this is a full access for car. This is, uh, this is, uh, expensive medications. So if you want them, go get all places. Bluetooth devices. Doesn't matter. And we are really, really bad at physical security. Then the internet of things, because everything needs to be online today. And that is a major problem because what can you hack? Do you have antivirus on get at home. No you don't. Toothbrushes the online. Why? When I started the presentation, toothbrush was not online. It was Bluetooth connected. You could buy a smaller ruler with the suction cup so you could put your phone on the mirror on your bathroom so you can record your toothbrush in real time and get real time feedback on how you're doing. That's a great argument for a toothbrush, not online. And I can also get achievements and compare you brushing others. Perfect. You can also hack it. It has not been seen yet. I hoped I had hoped it happened some months ago because there was an article about it. Turned out there was someone explaining it, someone who isn't studying and translating. But a German security researcher talked About how it's possible to have a detox attack from from a toothbrushes. It was theoretical and someone mistranslated and did an article about it, but it is theoretically possible. They just thought it had happened. But it couldn't be. And how about a box to keep X in? It's on Amazon. Perfect. So you can see how many actually have an A. How long have they been there. So are they going bad? Perfect. Why do you need an online tree? How about if you have online folks at home? The idea on that one is that people in my size, we are fed because we eat too fast. This one can vibrate when we eat too fast, and then you can of course upload what you're doing, what you're making, the calorie count and counting and so on. The business closed now. They did survive, but if you had $100 you didn't know what to use for, you can buy for a toilet. I've been waiting for that for some years. Actually, for four years. I can only on English, you can get in in Japan, but in English I can only find a Bluetooth connected toilet. Now they're finally here. So you don't have $1,870 on that toilet. Perfect. We have some on this particular, actually, but those are for. That's the things I mentioned. Those are for example, for dialysis. They don't have it sadly. But if you need to measure a patient's, uh, fluid intake and out put, it's easier to pee in a toilet than measure than pee in a cup. And people have to wait. So it's actually a good idea. But for home use, I don't see why I need a toilet with an app to control everything, and in the future I expect they expect them around to be 20.6 billion a year. In 2025, the value of the subscription market will be 58 million a billion. And for one thing, they expect they will be like 3.5 million such workers in 2025. In 2021, the number is still 3.5 million. That hasn't changed despite in Denmark, we have two new indications about this and it would be a massive upscaling security people, we still haven't changed the number. We just managed to stay sceptical. And worst of all, they expected to be 3.9 trillion IoT devices online. And remember we were 20. I said no one knows if they hacked this case 20.9 billion trillion devices. We don't know. No one knows this one. When I started this joke, three of the things here was online. Now, um, you smoke detectors on your alarm systems online, your temperature controls online, your doors online. You have hue, uh, bulbs in your home. Uh, you get on our toasters. I got that one last year. Uh, you have coffee machines online. Your dishwasher, microwave. My fridge is online. I can be. I haven't done it. Um, your car khakis? Yes. You Roomba! You robot. Um, what do you call a vacuum cleaner? It looks like it's liquid. Do you have one?

01:12:59  
*Speaker 2:* No.

01:13:00  
*Speaker 1:* Good idea. Because. Do you know what that is? It's a vacuum. It's great. It's also a camera on wheels. What can I use chemical wheels on? Two things. Uh, again, not a problem in my case, but I could see if I could get pictures of the people inside after they got off the path. One thing I can also use to scout. Do they have anything valuable before I begin? And now you give them a camera and wheels you can hack. Perfect. Uh. Trash cans. I have not found a trash in Denmark. You get online. I've found trash compactors in the US, which is more or less the same thing. And in Denmark, we're using them on the big public trash cans to see when they're full. So I consider that also done. The only thing I can find right now is a broom. I can find a broom that is little, uh, broom heads and can reach out wirelessly, but I can't find online yet. I'm sure it'll come, but I think it's scary that since 2017, all of this has gone on. And this is what I tell people what to do. Yourself update the software. Patching is the most important thing at all. And we'll talk about that moved then. Password database never reuse passwords as often have been owned. If you only use one password, one leak and I have you, your email and your entire, uh, digital history and access two factor and everything can back up. I lost nine hard drives in my time in it with data, and I could have used nothing major, but backup is a good idea. It doesn't matter how you do it, as long as you don't only have it in your home. I know people say, have I moved the the data over on a USB disk? So on on the USB disk. And if that dies, what happens? Oh yeah, backup is having two copies at least, and hopefully also one outside your home. Because if you have breaking a fire, you steal all stuff I have. I have a backup cloud in the cloud. I have a have Covid. You don't trust clouds? He has a bank box and a USB disk in there. He gets one month fill up data and put back in the bank is a little cumbersome. He works and then have it out to check because if you don't know you compromised. You can't do anything. You've never compromised. You can actually act on it and then think about your posting online because again, online, what about you online? If you Google the name, do you know? Have you tried that? It's interesting.

01:15:19  
*Speaker 2:* Yeah, I don't think I have anything on my name.

01:15:22  
*Speaker 1:* Who knows? In my case, I know what I mean. I do the test, I've done some translating on some comics, which means most of my hits are LinkedIn or on, uh, library sites or book trading sites. But it can be interesting to do. A good example is that I have a Gmail. Uh, the problem at gmail.com I was a user. The problem is five on the same country once in a while. I also think they have it so they use used. So I get their meals. It's all from, uh, our football teams, uh, new shirts, what colors we use to. Can I have my last year vacation in Australia or in case of bills? It's all in that level. One of the things I got was an email from one of the Danish. Um, we believe thing is not do something about helping foreign kids. Perfect, I build them. That's great because they send me an email with, uh, things about the joining the weekend and the 97 people who joined. They put them in CC, and if a company do that, they will get a fine you complain to form, which meant they will get a fine. If it's a fining, you can do that. It is actually legal. It's very bad idea, but it's legal. I checked and I emailed them and said, hey guys, this is not good and if I was on right wing idiot, I could probably use those 97 emails to do some damage. And so a month later, I got another email. I meet them again another month later. Come 30 minutes. Then I got pissed at them and I spent 20 minutes because I had the the email and the first name of those two peoples in the mails. 20 minutes later I gave them mail saying this way work. Here's your pictures. They both have Facebook profiles here, Facebook profiles. Here's where you live. Here's when you're on vacation. He's going to have to break in. That's what I did 20 minutes. I can do that. Everyone will please stop for now. They got the message, but it doesn't take much time because people do leave a digital footprint and you can use they can scan because whatever I can find, I can do a scam on. Hey, do you have kids? Perfect. Uh, the kids emails. Hey, we have the email. The email and the phone number can spoof. And we have. The kid is 16. Hey, dad, I broke my iPhone. I need some money for a new phone. Come on, scam works my coworker got recently. He don't have kids, so he surprised to get a 15 year old kid about his phone. But it works. The more data I can find on you first, the better, because I can use it. That was what I had. And then when he wrote, they started patching. I should have said, okay, you don't have to move. It doesn't matter much to me because patching is the most important thing you can do, and we move on and host it because again, it's mask and shield. If you don't patch your fault, they will get in. Our problem is our size and our leadership because it's hard to patch when the 2008 support. But we do know that if we try to isolate even XP for example, they are around. We have around 40 XP machines think they are isolated in their own behind their own firewall, or in their own area that is not accessed from anywhere else. We also have people who actually say, hey, can you get a machine to do that because the software doesn't work anything new. Uh, the psychiatric software, they do, it's proprietary, so no one else can make it. So we can't even make our own. Uh, you can take Nick. We can't machine. We just need the machine. Yeah. No problem. Of course do that. But, uh, we will try to isolate everything we can. And, uh, once in a while, we have to do. Say, what can we do? We have some reason to say we can patch it. We can stop it, because then we can't send bills to any doctors. That's not good. But we can limit the damage by saying, hey, at least only a IP address can access it. We've blocked a lot of the world. We've blocked Ukraine and Russia and China and India and around 17 or 18 other countries, for example. And then we open if people need access to specific sites or if someone specifically needed, for example, Ukraine actually need access to Redcap to do some work for Chip. And I actually could open it. And uh, of course we did that, but it's basically IP address. It's not the whole country. So we're trying to limit who can access. And yes, we are pissing off people once in a while, but we were afraid there would be a huge complaint when we blocked the first 12 countries. We've opened for around 70, uh, unique, uh, websites in two years. That's not a problem. And yes, it might be that one. Doctors mutated, but sorry, in the entire security is more important. Uh, in our firewalls, when someone tried to attack us, we will drop the traffic and say, hey, you do an attack, they will drop it. When we blocked the 12 countries, our blocked traffic drop traffic dropped by 70%. We didn't expect that one. We didn't expect that much, but it actually gave a lot of extra power via firewall because I spent a lot of time dropping traffic from, uh, certain countries. This is a big win. That's usually what I use when people are complaining about why we are blocking India, because it actually is a massive attack vector. Of course, if Russia went in, they don't do it from Russian IP addresses. No, but if you can stop 70% of our random scripted attacks, he would win a lot because sometimes they get lucky. Yeah. But patching is important. But again, if they get lucky, we need to secure it. And again, we can't always. But it is a massive, uh, massive focus away from us. Basically my department, we get emails from the center for cybersecurity, uh, CSIS, a security company in Copenhagen. This is some institutions, uh, SOC and sees that the American, uh, version of security and a few other sources about any breach. They learn of any CV to know about what CV is. And I can show you. It's very basic this. Whenever there's a breach, they will get a savvy number saying, hey, we have a problem. There's one here, for example, here, um, we just find it. Today we got a mail about this specifically, uh, where someone said that he. There's someone on the cyber panel, and this is the CV, the number, the security breach number. Basically, what you do is saying we're doing a lot of numbers and big companies like Microsoft, so they'll get a few thousand of 100,000, by the way. So you have them for this year's problems. And smaller companies will get random numbers as you go along. But this is the one where you check vulnerabilities. And this is also why I say, hey, there's this or that. Can we block that on a firewall? Perfect can is the windows based Microsoft Apart. You still have a few hundred CVS will go through and say, hey, we patch every month. But in our size we have over 3000. It takes a few weeks to rule out, so of course not on day one, but this could be bad enough. Basically they go from 1 to 10. It was good speeches 8.8 or higher. It's a patch now situation where we say, hey, now we need to patch if needed. Which means then we talk to our uh, uh, windows guys or the ones who sponsor a specific system. Redcap, for example, I want to ask windows about Redcap guys, so send it from there wasn't cheap. Before I go ask who he this specific subpart of a redcap. Do you have that? No. Not sold. Okay, then we don't need to patch, uh, the last patch Tuesday. Uh, for example, I had the we have role that goes, uh, on a weekly basis. Not a pattern, but vulnerability. Master who handled all of these cases. And I look old. Microsoft thinks that. Okay, I have 12 I need to talk about, and five of them is this specific software? Do you have that installed? No. Pivot don't care. And we end up saying, hey, we need to patch one is the same serve two zip servers. And that was it out of a few hundred because the rest is low priority. That can wait till we do normal patch, but anything important we will try to patch right away if possible. There will be cases where we can't do it. If there's a 24 over seven, uh, system for intensive care, we might need to warn them and say, hey, what can we do it, for example. But it is a probably the biggest and most important part of my department saying he we need to be in control of the patches because yes, you could. You will always be able to bring in. There is no solution. You cannot be 100% sure. Again, you could stop this building. Perfect. Uh, one of my co-workers girlfriend showed up and say, I need to talk to Burton. Okay. Go in. Perfect. I get Google and LinkedIn says, hey, I need to talk to my friend. Okay. Then you have access. And in Houston, sadly, we have not been allowed to use what's called NAC, which means that if you have pussy in that plug over there, that is this PC, no other PC is allowed. That's how you should do it. We have over 6000 PCs and a few hundred thousand pieces of medical equipment that are being moved around. We start blocking. People start dying basically. So we would love to get it. And my guess is we're at least ten years away from being able to do so. We can start saying, hey, that machine that's trying to attack us. Someone put because I walk through till I find a free plug and put it in a Raspberry Pi and use it to attack. We can block that specific Mac address from attacking perfect or this big port, but we cannot do a general thing. We do blacklist on the whitelist. I would love to avoid saying this is the only thing allowed, but we can't. That's one of these problems. As for what we do about handling it. Uh, let me show you. Um. Now, on the other side. Because we are trying and this is public health, I see many public information available for everyone. I would say you allowed to use that, if that helps you. Because every computer in Houston will have this, uh, shortcut on the desktop. Because in case they have, let's say we get ransomware, our entire network is down, and, uh, our boss say, hey, what's our emergency procedures other than the network drive? That's a very bad response. So basically, again, a cheap escape is here. What do people do? It's all documented. We tested every year. Which means, uh, what's in this folder? There's, uh. Yeah, about long term IT. Problems. Shortcuts to safety. Tips and tricks. Documentation. The phone book. How do you do? Emergency order? Anything. So say to the full list. Hey, here's a list of a phone book can reach people. Um, espionage scheme and saying hey, if if people need to work in a certain platform here, emergency schemes you can do and then put in the data when we are running again. Uh, and again every hospital. What do pathology department. They have had a requisition, uh, send two samples. All of this is down here, so everyone have access to it, even if the entire network is offline. Uh, we do weekly tests, are yearly tests and saying, hey, how do we handle this? For my department, we will have 3 or 4 people attending because we have a big part. And our A person, 3 or 4 more. Back in the old days, it was me. Nowadays, we're trying to change because my boss knows he can send me up and I won't have problems or be testing new people. But basically the saying he, how do we handle this? We'll do a test like, okay. Uh, internet bugs down. What do we do? Which means we talk to will appear from all the emergency area. So yes, there's one factor. What does anyone do? Because we use IP phones today. So if our neighbors down our phone system is down, how does 18, uh, 112 and 1813 works? They'll default to cell phones. Perfect. I was sure that working uh, uh, information. Uh, there's press contact. How do you contact the press thing was doing on it? Handle the phone account from the press. Uh, do we have emergency websites where you can. You can look up other things. We'll say, hey, we're down. We're working on whatever. Uh, do we have a press release already saying you can. hold it down. Um, let's say some stupid is important. Mask is a good example. When masking went down in a few hours, they had put in. Hey! We're down. Here's provision. Made an attempt saying what did we do? What happened? What are we doing? We had that in the somewhere and just pulled out the heat. This is what's going on and you need to have that ready for the person. Of course, there's nothing worse than saying, hey, we're done. We don't know what's going on, how, and we can't figure out how to tell people. Some years ago, uh, Facebook got hit by a nasty virus. Um, they were down for 30 days. They were down and irresponsible. A lot of things, including schools, libraries, uh, daycare. They had two guys every day taking taxes and cars around to all the schools, daycares, uh, the town hall, the whole thing. Putting up a printout of the day status Of course they didn't have any phone change. Anything ready? We have that. We were tested vigorously. Of course, we need really need to know what's going on CMT. We ought to have our own, but skip that one. You will not get a copy off because that might be proprietary, but we'll have a for example, again, Phonebooks from parcel we changed to personal our new phone system. How did that work? We have a I show you. I can't, uh, give you a copy. Thank you. Yeah, this just about fire. Doesn't matter. But again, we need, uh, what happens in case of fire? Of course you need to have it, but, uh, it's not interesting for us here, but it's still 31,000 pages is fine. Leave the building. Yeah, but no. Explain. What do we do? Who do we contact? Who shows up? Uh, communication. How do you transfer it with the again, for example, like this 12 hours maximum. Then you have to change the emergency details. Do we transfer the responsibility to someone else who handled it? Which department handed? So all communication, everything going on is fairly well documented. That is the estimate. Our services then improved. The procedures we we actually had with this building goes down for unforeseeable time. Our service desk and our desks will move to another location. We have. I can't tell you why, but we have another person who can sit and work at. And, uh, how did the cases show in our town? Uh. Henrico. This is basically my own. This is what do we do in case of emergencies, though? One for every department. What is their role and function? This in our case. What happens in the Beecham who found out? How did they find out? When did it happen? What's affected? What is affected? What is the damage? Does it affect daily running of your hostels? Have found the source of the attack. Internal external attack. What type of attack? We need to talk to. Who need to get involved in this one? Uh, then again. Yeah. We start at the track with our supplier. Will help us if needed. We do chain our anti-virus. We do check our docs. We check our email, we talk to TTC, our solution about, uh, our firewalls. When we have control over what do we do? How do we analyze it? So stuff like that is and how do we clean up after that is written down and again tested recently. In most cases we don't get that far. This is for big uh, it takes the big problems that will put the running hospitals down for days, basically.

01:32:23  
*Speaker 2:* Is it possible to get this, uh, guide?

01:32:26  
*Speaker 1:* You cannot get this one because that would be confidential. Uh, you can get the one for the hospitals themselves.

01:32:32  
*Speaker 2:* Yeah.

01:32:33  
*Speaker 1:* Uh, do you have access to we can Hope machine? Uh, then you have it. It's on the laptop or desktop. See this game? It's called footlocker. This. You will have it. It's an already have it as a default. Because every department based on their own procedures. What do they do if something happens? I had a good example some years ago, and we had to update our, uh, uh, Excel with our switch rooms where the switches go, which means we'll take the entire building offline for some hours, and we need to do it for the for the emergency room, which is not good. Normally we did on weekends. That's not a good time for emergency rooms. So we talk to the person and say, when do you want this done? And this is a night between Monday and Tuesday from 2 to 6. Okay. We'll do that. No problem. You need power or do you have power or.

01:33:32  
*Speaker 2:* Oh, just want to have it.

01:33:37  
*Speaker 1:* Doom doom doom doom doom doom doom doom doom doom doom doom.

01:33:41  
*Speaker 2:* You don't have. For some reason you might want to have it, but you can get a copy of this one. I have. Of course, we don't put the entire thing in the your, uh, papers, but you can use it to see what are we doing and so on.

01:33:58  
*Speaker 1:* Yeah, because I'm not gonna use any product.

01:34:00  
*Speaker 2:* Exactly. You just do, general. This is how they're doing. That is not a problem. You know what? I'm just going to do this. Two seconds makes a surprise. You don't have it. I thought everyone had it. It might only be the leaders had best me would have it, but I would rather make sure you have a copy. Two seconds.

01:34:27  
*Speaker 1:* Because I'm anyway going to send you the. The information that I know is okay. Revise it.

01:34:37  
*Speaker 2:* That'd be great. I would have to ask for that later, but it is not a problem.

01:34:44  
*Speaker 1:* There you go. Just going to get this one. $0.02.

01:34:49  
*Speaker 2:* Or 50MB. It might actually be to say let's see. Let's see what I can promise. Otherwise we'll do. I'll make sure you get it anyway. Uh, we have something called the hard drive. We can share files between, uh, people in those network just get removed everyday. So usually to say when you need a copy though, no problem. We have this one called feeder fixing on our drive, and whatever's in there, uh, can be seen by everyone and it's clean one in the morning. So we just put a copy there. If you don't get the meat, I can remember a limit for email size is just over 50. It might be the limit. But no, that is fairly standard. But again this is tested. Uh, but again, I used a few years ago and we cut the binge care unit. Again, we talk to their bosses. Perfect. There's agreement it was put on the internet. It was sent to emails to the department. You send an email the week before and the day before, just in case. And we talk to them saying, hey, we are now. We call them two months before because you said, hey, we're going to have one machine we're keeping alive. You just need to take off on two minutes and then to put a new switch, and then it'll be live. But we have everything and nothing else, so we call them and say we're going to do it now. What are you doing? Cutting into it. You can't do that. We had this green for a month and you can't do it. We have to. We can stop now. What's our emergency procedures? I should hope you know that, because that's not our job. Much later, we did it for the Heart stop monitors, which also include the same department. Exact same problem, including water emergency procedures. They had no clue. But every part nowadays need to have their own procedures. My wife's department did not have control of it. No, they found out that they had a lot of physical stuff lying around for it, and half that was expired, for example. So something the population need to review and say, what do we do if we do not have internet access or access to anything for a while? We have backups of everything. Of course, for some years we didn't have backup for our network drives, only the ill drive where we have the patient dates because someone said he the Pete drives, the entire department drives. And that's an important if you go to any of the department. If you drive Portland, they would disagree very, very loudly. Now we have bag of everything. You have space right now. The problem is with our data storage. It is ridiculous how much data we have. We have several petabytes of data. It is a to the problem saying, hey, how much physical space do we have to put racks with disks that we just bought new, uh, storage again for it? It's expensive as hell. We also trying to limit people and say, what should you do? Again, we are very open. You allow to use computer for personal use, but there's also several rules that we are also allowed to say, hey, you need to delete whatever we have. That's not work. We need it if needed. We had one time where we ran out of space on the personal drives. I got the job saying he figured out who's taking my space. Fine. That's my job. I did that. Uh, so I had to divide the people saying, hey, you have 300GB called backup of personal computer. We delete that, please. We have no space of 300GB called a summer vacation. Pictures. People do that. Or in one case, going to gigabytes of porn. That got it really fast. People do nothing about it, sadly. Again. Usually our biggest problem is a huge bias because they will click on anything to anything and not think of it. It's gotten a hell of a lot better. When I started, we were not allowed to tell you anything. Nowadays there's actually a video about it security, and we actually try to do campaigns as often as you can, but we are allowed one hour a year from time to time and you say, why not more? Because one hour a year times 50,000 people. That's actually a lot of nurses and doctors. That's why I'm not allowed more. My department would love to do a phishing campaign, for example. Of course, of course you do. That fish game is essential. Yes, and we have 50,000 people. Let's just say we'd be nice. We'll do 2 to 5000 people. Uh, have them don't check the mails because again, my wife, the first month she had got to work, we did meals. Our cleaning staff don't even log in to their meals. So let's say half. Don't think so. A 2500 people who check them out, let's say, have them fall over that. Don't fall for it. But it's getting worried. And call our service desk. Then we have 2500 calls to the services during a few days. Uh, putting pressure on everything, actually. And lead. Can't really do that. Or rather, we would have to call an extra, uh, people. And we can't just hire any time workers because they need to know our systems. So it is not trivial to do a simple thing like a phishing campaign, because 2000ft, everything usually has 300 people with no business doing monthly. But Nazar is no good.

01:40:06  
*Speaker 1:* Okay.

01:40:07  
*Speaker 2:* What do we have? Questions?

01:40:09  
*Speaker 1:* Yeah. So I have questions. How? How do you think that the cyber attack on a hospital and a dangerous healthcare system in general relate to the cyber warfare? Do you consider it as a global issue or the local issue?

01:40:25  
*Speaker 2:* Both a global issue in the general terms of money? Is it for money is global and we will hit like anyone else because people can do people's work mails on this. Because having owned again hey, there's emails, we get those lists, we attack people. But also uh, but nowadays we also target for attacks. Russia would be interested in making problems. We do see attacks from Russia. We do see deals text. We do see stuff. Uh, we have Iranians ticking down gifting some years ago. We do see a text from nation states. Uh, Russia is a big worry right now due to the Ukrainian Russian war, But I would say North Korea, China and Russia would be the three biggest threats we have. And North Korea is not so bad. I regard those are more hitting Asian countries, but Russia is a problem.

01:41:18  
*Speaker 1:* Are those cyberattacks more political?

01:41:21  
*Speaker 2:* They're very political. Uh, when? Because right now, if Russia we talked about the propaganda before, if Russia can get public opinion changed by the ball. Perfect. So if you can say put down the hospitals or the power supply or the water supply down, then people stop caring about the war because we, uh, care about our own welfare. Hey, do I have heating to have water? Do my hospitals work? Do my power work? If that doesn't work, I don't care about the Ukrainian war. Sorry. So can you disrupt that? Enough. Make a problem. Not that Denmark either need to spend a lot of resources changing it or have to give up or just say, hey, this is a new normal. Then people start saying, hey, maybe Russia is not so bad or Russia is. You think? Not that maybe you shouldn't provoke him. That's probably what Putin is going for and saying, hey, can I scale it is what is going forward. Can I scare countries into not reacting? So if he can scare, let's say threat of a nuclear war, for example, which has used, we can start saying, hey, I might use nuclear weapons that might scare people away from supporting the grid. That's what they're going for. Okay. We scare people. And part of skeptic would be cyber attacks on hospitals.

01:42:38  
*Speaker 1:* Yes.

01:42:40  
*Speaker 2:* Uh, earlier on, hospitals were was was basically a secret. People would not attack. You get attacked by random attacks because, again, I can open a private meeting because you know that or my work made on some list, but they would not go for hospitals. That's happened over a few years ago. uh, the hackers attacked, uh, German Hospital. They thought it was the university. Next door was the same name. And the woman died during a transfer to another hospital. And Interpol actually had that case Austin handed as manslaughter and say this is not a cyber attack. This was a non murder case, which means a hell of a lot more punishment for people. So the police is also upping and saying, hey, if you attack a hospital you risk killing people, which means this is a very more serious crime than taking place in the library. But it will not stop people. The even till two years ago, this kind of a again, we don't attack hospitals because well, there might be there we don't attack certain sectors that's gone. Uh, earlier this year there was actually a cyber gang whom you, one of the leaders, and say, hey, I'll buy support from you. We do that, check through your network and then you pay us half the money. They even said he. Fuck all our customers. We steal all the money. The honest criminal thing is gone now, which means hotels are frigging. That's also why we have increased our staffing and the investments in cybersecurity very, very drastically. Because it is.

01:44:20  
*Speaker 1:* Needed.

01:44:22  
*Speaker 2:* And we will get it. Question of when in 2015 to 2017 we were down with ransomware attacks every week. Me and my co-worker told us that it's just really made a lot of money that year in overtime, because we spent at least 50 or 60 hours a week cleaning up. After we got new antivirus, that stopped. But I'm not saying we cannot have that happen again. It will happen. It's a question of time. People do attack. We do see attacks, and we can. We have very, very good, uh, security. We. But things can't get through and we'll get through, especially since we have access as physical access to buildings, because it's a lot harder to attack when you just connect to that plug and don't pass our firewalls, because now you're on the inside and we can't stop it. If you're a private company with the own building and a nice gate, we have to use your card. You're protected. We're not. And one day someone will exploit that method.

01:45:31  
*Speaker 1:* Okay. Is there any strategy to kind of predict the attack to kind of like, see where is the weakest point in the organization? What are these points in your opinion?

01:45:47  
*Speaker 2:* Yes.

01:45:47  
*Speaker 1:* We are basically saying starting with data attacks, there was a common, uh, we get to take region, on a regular basis where we have some suppliers. I'm not allowed to say who, but they do fairly good on protecting us. There was one incident recently where we were down for 40 minutes or so. Uh, they used a new way to do that hadn't been seen before. So a normal automatic defense didn't, uh, trigger. So they had to do a little manual work. But in general, we are very, very, very well protected against DDoS attacks. Um, malware also, we have very well we have a very, very good malware protection nowadays. My biggest threat is it physical.

01:46:29  
*Speaker 2:* Security.

01:46:30  
*Speaker 1:* Because if I can get through 80% of defenses by connecting to a network, it is.

01:46:36  
*Speaker 2:* A problem.

01:46:36  
*Speaker 1:* And it's not one we can solve. We can only solve it by saying, hey, we're going to close every door on every hospital and have, uh, buses and people letting people through. And that is not going to happen because that would not be acceptable Or ethically acceptable because you don't need if you're in line from the emergency room with broken leg. You don't need to wait for Bowser to let you in. People could die from it. Basically, we can't shut down everything. The biggest take would be physical. Not physical as in the bombing, but physical to say, hey, I can access the network because now in the building and past the firewalls, we're working on trying to do some isolation between hospitals and so on. So if one hospital get hit, they do not get hit. But it's a work in progress because it also affects every program we run. And we have over 4000 programs in there. Who's done approved programs? Then there's all the other stuff people are doing. Chip, for example, you allowed to install your own programs. You're the only department in the region who's allowed to do that.

01:47:43  
*Speaker 2:* Okay, so since you mentioned the hospitals, I read on your profile that you're managing 15 hospitals and Yeah. How would you say that? Telecommunication between the hospitals can be affected with the cyber attack. So, for example, I know that the chip we work with different hospitals in all household work. How would the telecommunication can be threatened?

01:48:09  
*Speaker 1:* Very easy. Uh, because we switch to IP phones. So if our network goes down, so do our phones. Uh, we've recently moved to puzzle our new call center, which means is in the cloud. And, uh, that we have just opened so we can access it, uh, from outside. But basically, before we did that, if you hit the hospitals hard enough, we would not be able to access the call centers, uh, control systems. If we could accept. We just couldn't log in. So if you logged in already, it would work if we logged out. It would stop working for the person. Nowadays is in the cloud that we've opened. So if we say hey and we did that recently, to be fair, again, this is not a competition. But we had an attack last month, I think, where we were down for an hour in this building. It's not.

01:49:00  
*Speaker 2:* The region.

01:49:01  
*Speaker 1:* To the massive data stack. And to stop that we said, hey, we cut all Nadine's traffic and then the consequences because Denmark is our primary customer. So if someone outside Denmark can reach us right now, don't care. But that also means we cut off our cloud solutions for antivirus, our partial call centers, and so on. All our cloud service over 65 and teams started working to do that. And we of course looking into can we open for these specific networks and say, hey, this is the big red lever we shut down, but we will still keep these servers open. And that's something we look into. What can we do about that? But we you don't see the problem before we pull the lever the first time.

01:49:42  
*Speaker 2:* But would the patients be affected directly by the cyberattack or will only the organization suffer? So what will be for usual citizens?

01:49:52  
*Speaker 1:* Usually if there's a cyber attack, it depends on how it hits. If it does attack, don't care. We do not have any stuff on our normal websites. That is. Of course you want to go to hospital. You can see the map or see the contact info. Do I care? No, I do not. A temporary problem if you are. If you name it, it's a big problem. You will press down for a day. In our case, we don't care that much if it comes down for the. Yes, it's irritating, but is not something that kills people. If someone's platform is down for the it's a problem. So if the attack is on our outside websites is no big deal. It's of course on the project, but is not not critical information. If the overload network like we did in the last eight hours, it's a problem temporarily until we get work. It didn't hit any patient systems, but again, it hit our ad. Actually, it hit all the instant communication. So systems that was online. Stop working so you can get hit a little bit by that one. But uh, again that's something we have fairly control over. But if you take down the phone systems, that would be a problem. We will default to, uh, cell phones. Problem is, we do not have 51,000 cell phones lying around. Uh, saying, hey, we do that once in a while. Departments that you can just get 50 cell phones lying around. Yes. Of course, if you want to pay 50,050 cell phones, 2000 of the phone and the monthly fee, and then they are not interested anyway. Of course, it will be seriously expensive. On the upside, a lot of, uh, employees do have work phones, which means there will be a part of the employees who will still be able to do work. And honestly, uh, right now, I have a company that'll change in a moment. And calls in Denmark are free to matter if you use your personal phone for work call if the network is down, does not it do not have any effect on you? Economically it might be mutating, worst case, some unknown private number, but it is no big deal. Most people will have a cell phone on them. Not everyone, but most will have. But yes, it will give some problems because you can reach the people on the other end and we have some in. I will skip the one I send you. There is full list to contact all our partners on the meeting. So on. How do we communicate? It's not perfect, but we have some ways to get around to contact each other. There isn't a lot of emergency fund, so yes, the main numbers will still work, but you might not be able to reach specific department on us, but you will still be able to reach the hospital and people cell phones to work. If the cell phone system in Denmark goes down, that's not entirely. And that's also not a that could happen. And then it's out of our hands. We can't do much. And if that happens, we can say, hey, we have to wait for Tennessee to get up and run. We can't do more. We can and do also have some radio communications with the senior radio. I do not know much about it. I know we have them. I know in our SOC, our service to dispatch a feature and a service to our services. But the next step, the dispatch case. And get all the calls if there's big problems. They do also have senior radios who communicate with the ambulances with the Gentile and the other, uh, senior. Working systems in Denmark we coordinate with, uh, southern states. So there is a coordination about that in general, insisted I think about it, the basis I'm not in it myself, but I know they're testing. They're basically scenery is not very good. It is an emergency feature. So basically stuff like he now we take 15 minutes of a month to practice same numbers on the radio, so be sure that the person get the numbers correctly. It's that level you go into because people actually fuck that up.

01:53:53  
*Speaker 2:* Okay. What would be your responsibility while there is a cyberattack on CMT? What will be the protocol of emergency response?

01:54:05  
*Speaker 1:* First, we would of course try and see what happened. Uh, my partner would be the most likely candidate to look into it because we are operational security. We will start seeing heat. What happened? Where does this happen? If it's a data attack like the last one? You guys and our supplier, I'm not allowed to mention them, but. So I'll say supplier. But they will look into our data. Is that where it's coming from? That could be it. If it's a virus attack for some sort of reason, it'll be my responsibility as an enterprise man. We will. Then we will see. Hey! What? What? He does. What can we do about it? Um, if you have time. We overtime. But I have time. I think you just see my calendar. I can show you. I have plenty of time. I need some power. Two seconds. But I can show you if you want. Yes, sure. You will not be allowed to get screenshots of that. Uh, if I need power. Do you have power in your field?

01:55:02  
*Speaker 2:* I don't have a power plug, but you.

01:55:04  
*Speaker 1:* Want to do it, otherwise you don't get it. I, of course, didn't bring it. Perfect.

01:55:12  
*Speaker 2:* Yeah, try this one, but I'm not sure if it's sufficient. The power.

01:55:16  
*Speaker 1:* We'll see.

01:55:18  
*Speaker 2:* Oh, but if you just keep it running, I'm happy. Let's see. What you.

01:55:25  
*Speaker 1:* Say. Hmm.

01:55:34  
*Speaker 2:* Good question. Yeah, I.

01:55:37  
*Speaker 1:* Just.

01:55:40  
*Speaker 2:* I just need to go.

01:55:42  
*Speaker 1:* Oh.

01:55:42  
*Speaker 2:* I have to. Two seconds. There you go. I think it's keep it running. Perfect. Now, what we would do would. In our case, again, I can show you a screenshot. I can show you what we're doing, because that is basically what we would do. So no big.

01:56:00  
*Speaker 1:* Deal.

01:56:02  
*Speaker 2:* Basically what we have in Houston is an extra resolution, which means we can, uh, see everything that goes on on a machine. And I do mean everything. Um, have you read the rules about, uh, who is the best in Houston? Basically, of course, we do not spy on you what you're doing, but we, of course, have lots of everything in case we need to find something. So, no, I do not see what they do. A machine, but if there is a legal or security reason for me to look into something, we can see exactly what has been done. We cannot see what we can see. What websites you visit. We cannot see any subsites, which means, for example, we go an extra. I can see the text, but I cannot see what articles are read. But I can see the hit on extra blurred. But anything related to your machine we can see. So we will start seeing hey, if this happens, if we attend users who say we got malware, we look into those PCs, see what happened. Let's take an example. And this is as long as you don't use details on this, you can mention it, but you can't use specific details because we had an attack last week, not a big one. But when I say attack here, it is not a problem. That was serious, but serious enough that we spent some days handling it. It was not an attack. Assault with someone trying to steal data comprises. But sometimes, uh, just need to make sure I'm getting power here. I am perfect. Sometimes when we get when people serve on the net, there might be a banner and master download that you noticing that can happen that do happen. Once we had over 500 people who had a specific file downloaded, they didn't download. In that case, we can go and delete it. The one we had here is that, uh, we saw a specific, uh, open source office, uh, program called GPS is what we call it, which was if I'm working soft and official Chinese, uh, company. To be fair, that is not a bad program. It's not an illegal program as track damage, but it's one we do not like because technically they use cloud solutions. Which means that if anyone open a document might have patient data, it might be sent to a Chinese cloud. So no, first of all, you're not allowed to install programs. That's a big No-No. You need to ask permission for programs, not from software job. On the ownership. Yeah, but, uh, this one, we said that we don't like it. So in this case, we start saying, hey, this specific program running. Uh, saying, where do we have it? Dum dum dum.

01:58:59  
*Speaker 1:* Dum dum dum dum.

01:59:07  
*Speaker 2:* It was in this case right here, the User profile, AppData Local Software and doing our job data. And it was trying to be persistent. So if you deleted it it would reinstall itself. That's why we got it. Because we don't like programs. We don't allow the trial to install itself. That is malware, potential malware. So we kill it. So in this case we wouldn't say hey, these machines, uh, could isolated, uh, and we, uh, get them reinstalled just in case. And now we actually have a check, this check saying, hey, if we see. And where do you have it right now, if we have an alert saying we have an execution where the signature from the excusable file is from a Saudi king sort of software and not on Linux, we get an alert on the machines and then we can handle the situation. That's a simple one. And if I need to do something, I would say we use my machine, for example.

02:00:11  
*Speaker 1:* Uh.

02:00:17  
*Speaker 2:* Because it's good. Because then you can see what we can actually do in terms of protection. And this goes for all machines. If I am worried about my machine, machine I will say isolate endpoint. Why do we do that? If we. If I trigger this one. This machine is in 10s cut off from being online. We can access from this tool so we can get full access to all files, process everything running on it, but it cannot spread in the old days. Uh, if your machine convicted, you would call us. You were worried about something. You call us, we'll say, turn off the machine, pull all the network cable out because people might not again put a post-it on. People should use it. And we set up a on site guy eventually. And, uh, ten minutes later, someone. He'll be running again. We had malware machines that got turned on again because people didn't see the post. Nowadays, isolate and our services can even do dispatch. You can even do it. So if there's a case two in the morning. But, uh, one of the users getting a weird pop ups doesn't say it might have virus. They can isolate it. We look into the next morning. So that's kind of how we handle PC situations. Say we can do it. If forensics like saying, hey, what actually happened? Which is important because it's fine to say we stopped it. But what actually happened? How do we do it? You can go in and.

02:01:41  
*Speaker 1:* Say, let's see. Dun dun dun dun.

02:01:45  
*Speaker 2:* I'm not perfect for this. I'll say I'm not a programmer. Uh, you can program this in a whole code language. One of my co-workers is really good at it. I have a program 20 years. I am not a programmer. But basically, this is what you can look into processes, files, network event logs, and connections. All of this is what we can look into happens in machine, uh, which means we can see very, very specifically. What did you do? What happened? Uh, we can give an example. Um, we had a coworker.

02:02:17  
*Speaker 1:* Um.

02:02:19  
*Speaker 2:* Whose contact is because, uh, the person's, uh, was in the movie theater, and, uh, there was a mistake on the person's Facebook that she did. Oh, sorry, she did not send.

02:02:31  
*Speaker 1:* And the only.

02:02:33  
*Speaker 2:* Machine she has was work machine, which was in her apartment with her kids, two and a two and four years old, and her ex-boyfriend. It's not hard to figure out what happened, but she wanted proof. And my coworker, he looked in the firewall logs and we can see. And when our lady would say, hey, that machine could turn on this time and then connect on Facebook at that time. In this one, I can say, turn on this time when the Facebook at that time it started the following programs. You do not save any files because he might have seen something on Facebook. I don't care, that's personal problem. But let's say he also downloaded some files or send email her name and then it did save files. Stuff like that. You could say, hey, Tim's items. He opened in explorer, open Facebook. That's all that happened. So we can say limited damage. Fair of no problem. You need to talk to him, but no damage done. But we need to go in and see exactly what happened a given time. Uh, let me see if I have it still. Um. Two seconds. I did a small, uh, teaching recently.

02:03:40  
*Speaker 1:* Um. Bom bom bom bom bom bom.

02:03:45  
*Speaker 2:* Do you do the teachings regularly?

02:03:47  
*Speaker 1:* Uh, the ones I just went with you around. If it's two months, whenever people need it. Basically. And we had a lot of people. So it's neat on a regular basis. And one of some of our people wanted on a, one of our 2 or 3 of our departments and infrastructure. Uh, basically people who've been for 20 years who don't think security also wanted. So I showed it to them and say, hey, this is what we can actually do. They were surprised, especially about this one thing. You can see that much? Yes, I can see exactly what's going on. Again, I'll be able to see exactly within the machine. I do not want that because a nurse do not want to be surveilled. 24 seven no, we do not do that. But in case of a security problem or B, here is a serious problem we need to solve. Or there's a suspicion of, uh, some sort of legal breach. Uh, so say, hey, you're stealing. Stealing? Let's say you're stealing files for this platform. Are we going to say, hey, what file? Which files, for example. Uh, do you remember the case? How long have you been in Denmark?

02:04:52  
*Speaker 2:* Uh, for two years.

02:04:54  
*Speaker 1:* You remember the case about the 13 year old girl, uh, who almost got raped? Yeah. Uh, there we find some people, uh, due to that one, because some people have been looking into the journal. They're not allowed to. Oh, yeah, we were one of the parties involved, and we figured out that it shouldn't platform. They can, of course, see the logs in there. So some people got either freed of suspicion or fired from that one. But some people said, hey, this problem is logged. But The emergency response platform for ambulances. I'll log in there and check instead. And then you go way, way past. That might be an extent to this is very well delivered. And we could see and say hey they want one of these signs. This is what is in the browser logs. This is the fight room. This is HTML file zoom that we can see everything on that one. We spent three days on it, but that got a few people fired because they made some massive privacy violations. So that stuff continues to fall. And where did I put it to? I'm not sure I have that specific document on there.

02:06:00  
*Speaker 2:* See that statement? Uh.

02:06:05  
*Speaker 1:* This one might be interesting. This isn't a case where we actually almost went in to emergency mode. Two seconds. This is fine. This is not proprietary. It's just a fun instance. We used to show people actually about what we can see. But we were this close going out with a baton hitting. People actually know something called a robot dog. You ever heard of that one? It's a small hack tool.

02:06:31  
*Speaker 2:* And.

02:06:35  
*Speaker 1:* It can basically do everything. Speed, robot.

02:06:40  
*Speaker 2:* Dog and.

02:06:42  
*Speaker 1:* Connect. It looks like this small USB device. And if I plug that machine, good luck.

02:06:50  
*Speaker 2:* Basically.

02:06:51  
*Speaker 1:* I can do anything. I can keylock, I can hack and do anything. Uh, if you buy some of these, uh, add ons, ten, you can use it to, let's say, hey, you're in the elevator. You happen to get near my pocket for two seconds? Now you have my card. You do cartoon stuff like that. It's fairly dangerous stuff. And we got an alert saying, hey, we have a problem here.

02:07:17  
*Speaker 2:* And, um.

02:07:23  
*Speaker 1:* But I'm showing here because, uh, the data only stays three months in our systems. Uh, so I can't find it. But basically, there's something called micro check that is a framework on how do people take basically until around here. Here. It's not that bad. You start going over here, it's going to be a serious problem. But basically, if you can stop anything around here, you're happy. This is exploitation. That's part of something stealing data. But if you do malware, you really want to stop around execution. But this one triggered reconnaissance, which is usually port, scan or duplex on the wall and try to check for IP addresses or availabilities. Initially I charge something. Exclusion. I ran something to the installation. I tried to hide myself, couldn't access, try to use admin access, collection and gathering data. I'm copying data to get all of this at the same time on a computer in Houston. We didn't like that. And it's a small robot dog like this. You can do payloads, passwords, exploration, key logging, whatever you like, basically. And we have four people on it.

02:08:35  
*Speaker 2:* Um.

02:08:36  
*Speaker 1:* Our problem is, as usual, contact users. We found out the user affected the laptop, so we didn't see the need to send out someone out to get her. At first we were afraid someone was trying to steal her plug in somewhere to steal data. Okay, it's a laptop and the user. And after five calls, I actually, because I was lucky enough. She didn't have connections, but the part she was in, I actually knew the head nurse, so I called her and telling me that she was at another department moving to them soon. But I can try these people. And four people later I got her close co-worker who tells me she's not. She's in an hour. Okay. She's not in yet. So it's not in the hospital. Perfect. Then it is either Sean or the husband. Because this is not something that happened randomly. And if it's on the home, it's on a husband who was playing around. So we talked to her. And we are in the place that we're talking about possibly involving the police and so on. If it had been something, uh, and, or a written, uh, call, the personnel say, okay, you get a basically you will have to give you a written warning.

02:09:46  
*Speaker 2:* Like personal.

02:09:47  
*Speaker 1:* Exactly. Exactly.

02:09:48  
*Speaker 2:* Yeah.

02:09:49  
*Speaker 1:* Basically you do that, but when you find out, okay, if this is a private matter because it's at home. And her husband, engineer, perfectly known as the husband, because that's not uncommon. It turns out that in the home Office, they have four docking stations and four, uh, monitors connected by USB wires. And she plugged in, and then he is trying to make a new keyboard homemade keyboard, which use the same chipset and program as the rubber ducky. And because the USB connector device is the trigger warnings. So we didn't have any files on his machine. But because this one say what you see in network, I try to make it myself as a keyboard and as a few other things. It made warnings on the machine, and we can see that as good as what we can actually see. And we see a lot. Uh, I talk to our firewalls. So once we connect to get, uh, collect, collect and collect data from all sources. So nowadays is not is advised on this. No. I see some fun things on my firewall. At the same time, this machine do fun stuff. Okay. That might trigger one. Would not normally see stuff like hey, I use data out of the house. We get warnings if you send out. I think there were 200 bigger party. We get warning. The problem is we don't have a. That's something we are working on. That's not confidence. You can write that if you want is decryption use SSL, which is how it encrypt data online. And uh, I'm not sure how it is now, but a few years ago, 60% of all communications worldwide was SSL and hopefully higher. Now it also means we can see what is actually being sent. So you have malware. I want to connect to something. It'll use a little to contact something. If you want to send data out because you try and steal our data, you use it to hide it. We're trying to get decryption so we can see what's in the data streams we send. Again, we would not. Basically I would not be allowed to look into the data stream. We our software I would say are from friends. We give it saying, hey, if we see.

02:11:57  
*Speaker 2:* You see.

02:11:58  
*Speaker 1:* 8 or 10 instances of a CPR number in being sent here to a non-secure address, uh, that's not good. We better trigger warning, but we would not actually be allowed to see the data. Even though we are skilled people and we have the what to call the security clearances. We are the second highest security clearance, but we'd be able to see something else going on. But that is something we're trying to get allowed to do. We spent ten years on, and so far I think I did with the guys before we had asked, tried with the new doc, but we're hoping to be allowed to do it now. The problem is usually that the security we can look into what people are doing. Again, people are allowed to use this privately. Can you can you see what I'm doing to my bank? Can you see what I'm doing about the ICO? That is usually the problem. And then we have to make decisions and say, hey, we know banks, there's a filter for that. Hey, we don't want to see financial institutions, we don't want to see healthcare institutions, stuff like that. But it is some issues you're trying to focus on. If people are stealing data, I can show you an example. Um, two seconds basically. Do you have the extra time? Yeah. Okay. Perfect. I just don't want to keep it if you don't have time. I don't have time. But there. Are two things you need to lock in. The other one. This is one we are also implementing right now. We have we have some small issues with performance I'm hoping to solve today. The list. I promised they solved it, but it's a problem we had before. Which means I'm less warning. I got this four days. I'm supposed to get 7 or 8 at least every day, so it's not working as intended. But basically we do right now is that we have a small system called the Cloud Manager, where we go in and see what do people actually try to send out, and what do we put on the OneDrive and the SharePoint. Because if someone has a SharePoint or have some bias and we would actually like to know it. So we have wildfire, which is the same database as our antivirus. Check all files saved in OneDrive or SharePoint and saying, hey, do we have a problem? Right now we have 390 problems. The problem here is that this is a manual sorting because antivirus filters say this is a problem I don't necessarily agree with. It's a simplified example. I'm pretty sure you would agree with me on this one. My PC backup set up. Yeah, you're not allowed to have that. You're allowed to run programs at all. So this one delete. No problem I don't care. The user can complete the one that's not an issue. But, uh, let's see if we found something. That was hard for them, to be honest. That's something we made meet ourselves. That's a PDF file. Why is that trigger as a warning? I can just delete it. It might be critical. I need to log in. Download this file instead. Why? It is being triggered as a warning. For example, I know that some of the other schools in Denmark, uh, used a link shortener because they don't like these long links in the PDF files. Fair enough. They used a Danish one called Short Link. That one is not that great and is triggered as a potential risk in many places, which means any PDF document using who has a link somewhere in the document using short link will be flagged as virus here. That don't mean I'm like I'm deleting it. It means I need to figure out why I should improve it. We had some students at school who had to use that one. And, uh, she's working with 15 people, and they had that one attached in the mail and started sending mails to each other, which means 15 people in CC every time give me 15 warnings or spam filters every time this reply to it. And I had to write to them saying, hey, please stop sending that file because it's a problem, but stuff like that, we'll have to look into and if we have the other one is, are we sending out data and it's not working yet? Perfect.

02:16:17  
*Speaker 2:* It's from external.

02:16:19  
*Speaker 1:* If we're sending out data. I'll take an example. And I can use this one because there's no patient missing that one. Because what we can see we can not see the email. We can download the file. If it works right now we have problems. But we could download the file and see what's in it. But we can also see why do we have triggers in this case. We have a teacher. If you come here teaching you will have of course need payment. So you have only reason to know what. And of course to do that we need the CPR number that we send that to the person. Of course we will set that to is too difficult because you need to get paid. That's not a problem. So this wanted to say, hey, we're sending it with a source we don't know. We have what is called quoting. Do you know, that one basically means that around 3000 domains in Denmark is on a network where we update on each other. So if you meet Reagan, who's done MIT in Houston, it's automatically encrypted. But if you email someone not on the list is potentially possible to read it. So it's a trusted receiver. Hey, and fair enough. But if you're trying to, for example, a doctor sending a privately, if you add, you post, you download your journal from a Sony Echo. You allow to do that, of course, and you send it to your own game. That's completely within your right. Of course it is. But if you download as a doctor, send your patients journal to your Gmail, then you could pay for validation. And that's what we look into and say, hey, do we send something out? In this case, not a problem. You're allowed to do it. We only check on CPR number because there's a lot of checks and ten numbers. Is also driver's license. Bulgaria. I don't care, and we run into a lot of problems. We'll also run into, uh, again this American filter. So, uh, profanity filter because people might curse, which means stuff like slut, which it will trigger a warning, a little warning. We don't care about the warnings, but because we what we should see. That's all we look for right now. But if we have a case where a doctor sends his patients data out to his, do you know that it is the doctor's union? The. If you a doctor or a member of the union, you get an email account and all private practicing doctor will use it, and none of our doctors use it, but they're not allowed to to send our data to it, and they don't really understand that. So sometimes you need to tell them if Doctor Dude wants, I'll call them and say, hey, by the way, violation. We don't. It's a one time thing. We don't need to make a imparting to Jonathan Stills and so on. But he consider don't do that. But, uh, I had a doctor who who had a secretary in another department, uh, package 12 journal files with the time stamps with nine month period. And since he's done it, that is not a single time use that is showing you have a a method saying we are sending only nine journals to my email that went to the lawyers because they need to talk to him in the morning because that's actually about average. That's big enough for us to handle. So yes, we will look into stuff like that. But no, no one is interested in seeing everyone send mail. It's only the trigger. Initial warnings. We care. I had one once. Where, uh. Uh. Professor. Yeah. Again. Long education. She fell for a meal for Norwegian about the 12th. That one she sent to her husband, who's a lawyer again on education. He also fell for it. And his reply about where they had to go when Banfield also had to call both these guys who have combined education three times and might tell them, hey, you idiot. And that is.

02:20:20  
*Speaker 2:* A.

02:20:21  
*Speaker 1:* And normal thing in here. Education length don't matter about security. There's absolutely no difference if you're working as a doctor or in the clean department. They are equally likely to make followups basically. And again, we are very nice. We don't fire people. We don't, uh, do anything bad. But you have to basically break the door for anything to happen. Uh, it do happen, but it is very, very rarely. I had one case some years ago where they shared their logins, Elegance, which is the problem itself. And they did it because they're bored in the night shifts, and they put all the pirate copied movies on this person's personal drive. And on that drive, they also had a list of what they could sell, copies of the DVDs and the 600 copies for the movies, and we could identify four people involved in that. And those four got a written warning. But you need to get up to that level in med school to be fired immediately. And here we are. Nice.

02:21:26  
*Speaker 2:* Okay. What else.

02:21:28  
*Speaker 1:* Do you.

02:21:28  
*Speaker 2:* Have?

02:21:28  
*Speaker 1:* Uh, who are the main victims of the cyber attack who are suffering most from them? So, for example, if a nurse get a, let's say, phishing email, she clicks it. And which data will be compromised. So, for example, most people have the outlook on their PC outlook on their personal phone. Is there any connection between the PC personal phone contamination?

02:21:58  
*Speaker 2:* No, we actually tried to separate that quite easily. I have a work phone we allow to use privately it actually so that, uh. And we've installed it on my private phone. It makes two profiles, a person and a work phone. If I take a picture on my phone and then it seems to my coworkers and it's the teams, I actually have to go in and allow my phone to get access, uh, to my personal, uh, area to get the file. So phone wise, we have a fairly separate, uh, system. I'm not saying it cannot is not possible to break, but I'm not worried about it because there's fairly good software in place. And, uh, in Asia I would worry because in Asia, they tend to jailbreak their phones and not pay for the apps and thus get infected. We don't really do that. We don't. We protect our phones from jailbreak, which stop most of the problems. If you need to infect your phone, you basically need to really get on log in something Google or Apple missed in their shops. You can install other shops if you get a PDF file or some bad stuff in it. No big deal on the phone. Actually, if I get a PDF file I'm worried about, like this one. I'm not a human on this machine because that might comprise a mobile phone because they can't really hurt anything there. But if the infected machine, the worst thing is if the two enter key logging or give the login away because then people can log in and start see what do they have access to. And if you log in, they'll have access to your email. Of course, if they know enough to get in the physically able to get in here, the access to your network drives which keys again in need of help. But no offense if I walk into Chip just like this thing from an IT department. I need to borrow a machine. I'll most likely be able to. And that goes for any department you can plug you into almost anything. I can get access to a machine and have the someone's login. I have access to all the documents and then I can start stealing whatever they are. If you can do that a lot of extra sort of platform and be able to steal data, it will be locked, but I will have access to it. That is especially a problem because many places they don't care about locking up because I'm just doing machine for ten minutes. My wife's department do it and she's trying to tell them if. Yeah, and the patients have access to the machine, if they look anything up, it's in your name. You're the one getting fired. That's the problem. In general, I'm not so worried about the nurses. What we've seen so far have mainly been ransomware attacks or again, emails. And yes, you can have some sense of emails, but you're not allowed to have patients mission emails. What they can use. What the be interesting to see here is if I infiltrate someone from the finance department who handles all the contracts. If I use that and send an email to the department saying, hey, by the way, I'm from Siemens. We have a contract and this contract number, we have this information. We've changed banks with the new numbers and change that. That won't be. And because you have the contact numbers from the email, you can fake that and you will not notice it before. Siemens was asking why they don't get the payments anymore. I see that's the economic problem for the patient information. You would need access to a machine. Also also need to break the rules because if you use VirtualBox plus our solution, you will need two factor to get in. So then you have to get the phone again. Potentially you can hack a two factor and get the SMEs somewhere else. I don't do this with views. Uh, I don't allow a mis two factor. We use, uh, interest identity. So you basically can't. You will need access to a phone and a machine to do that. But again, if you can blow off my way into hospital and do something against the patient data. Yes, we are not allowed to stop, uh, USB devices so I can do it with the USB device. We have the extra two USB devices from our systems, but if I do that, will any USB device, a medical USB device stop working? I don't know, need to be tested every system, so that is not acceptable, sadly. Because I can damage a lot very fast. I'm also actually worried something about the killswitch if you know that one. If I need. If I don't want to steal data that's trying to destroy something. Yeah, the Russians could put a bump on our cables as a joke before, but, um, again, if I brought my way in to the department, I have a USB stick. I put it in the USB device. It receives powerful USB device for around three seconds. Then they send the power switch back as far as the motherboard. Um, cost around $100, and if I do that in 20 machines, go to the next hospital. I can do damage for millions. And who can stop me because we don't have video surveillance? We don't really blow off and plug anything. I can go in and do that. And the only way I can stop that is by saying, hey, laptops. The we need to glue a keyboard and mouse to the laptop, put epoxy in all the other USB ports and through the laptop out if it's one of the dies. The only way is to protect against it. I'm worried about that one because we can't protect against it. There's no way to do it. As a patient. Obviously I'm more worried about the individual person's data if they get hit, because again, we've not seen many we've not seen examples of patient data. We've seen ransomware. That's irritating. We will eventually. She went to a tragedy later. It's a question of time when it happens. So I'll say there's no silver bullet. It will happen eventually. Someone will have found a way to steal something. I'm more worried about the consequence of the individual news or something clicks on link because again, the if they get extra on this platform, it's their job. If they have enough incentive and the emails have access to it, I can do a lot of damage. If I said before me not stupid, even stalk someone if I can access to the email. Hey, perfect. We have seen situations where that have been used in emails, with fake porn, pictures to coworkers and so on. We have seen that done sadly. I'm more worried about that part because that is also a security in it's a good thing. Not my problem, but ethically also. It's also our problem to help our users. How do we handle situations like that? Because they do also happen with the number of users we have. It happens once in a while, sadly.

02:28:43  
*Speaker 1:* How about the mental aspect of the problem? How dangerous is the cyber attack on the mental health of the employees? And for example, a doctor will be worried about getting hacked so the patient cannot get the treatment in time. The operation. What about.

02:29:04  
*Speaker 2:* I would say the general doctor is not worried about cyber attacks and such, and we have our emergency plans. We send you the the people who do that worry about what how do we do? And that's why we test and practice. How do we handle it? The real doctor would not be that worried. In general, they might be worried. If you see the news. Okay. Something's going on. Be set up. Cyber security increased the evaluation to very high. It does some mental worries. We have had situations where people get paranoid and do stuff. Um, I had one which I think at the moment I talked to him. He had to reset two phones, one phone over with, uh, some sort of, uh, machine. And, uh, he was worried about hacking that he had an old Nokia non-smart phone, and he thought it was hacking because it started blinking whenever he would go towards the airport. Sometimes a worry can lead to paranoia in employees, and that's, again, not my problem. But since it involves it situations, we will try to do as best we can to help people and say, hey, do not be worried.

02:30:14  
*Speaker 1:* So how would you ensure them in their safety and would you provide some training materials?

02:30:21  
*Speaker 2:* We would normally not be allowed to train outside. Stuff like this is internal and same thing again. You were asked permission ask specifically. Of course we do it, no problem. Normally would not do it. But in a stuff like the CEO Ford thought I spent five minutes telling people what happens? I made a small, um. Let's see. Where do we have it?

02:30:47  
*Speaker 1:* Two seconds.

02:30:55  
*Speaker 2:* I made this small one about the CEO for central people to say, hey, how does it look? Just as he. This was what happened. So basically, whenever people are either hit by zero fraud or I can see they got someone attacked, tried to attack them, and we get into spam filters. We know, hey, you are now a target because they didn't see you. It will happen again. So I'll talk to them and say, hey, do you want to cover this one? Because then take it up and they're in a department meeting and say, hey, by the way, we've seen attacks on us. Uh, you need to be sure you don't, uh, transfer money as you talk to me, just mention it and use this as a as an example on what happened. So we can show people that. But you do not do a hardcore training loop. I'll do some examples. I'll talk to people again. So the paranoid ones, I will try to tell them what happened. What can we do about how can protect yourself stuff like seeing it have been out and so on. People do that basic stuff. We'll do that. But no intensive training for individuals. Sadly, I would be very happy if we someday actually had some sort of training. People start. We do not do that. We basically say, oh, by the way, you have one drive and you have P drive. Good luck. And you could with some probability you. And that's what happened when I started. And it has not improved in over 20 years hopefully someday. But the problem is that is the individual patterns of responsibility. So we can force them. We can do one hour a year training videos and we're trying to do some other departments. You've done some training videos to explain a little about what happens. That motif don't really know that we have some lying around where we're trying to do. You can probably find them online on our internet, but we actually done a few videos saying, hey, the fishing example is how fishing works is what you do about it. You're trying to do a 2 or 3 minute videos about it between 2 or 3. So far.

02:32:53  
*Speaker 1:* This is public or private information.

02:32:55  
*Speaker 2:* That is, uh, internally in holes that you will not be able to use. You can mention we have it, but you can mention details from it, but there's nothing proprietary in it. But you I think you probably I always say those videos you could probably send put in the if you want to use them. Yes. You can find them to send you. Would you be able to allow to use them? Uh, there's nothing sensitive in them. It's.

02:33:23  
*Speaker 1:* Uh.

02:33:24  
*Speaker 2:* Yeah. Okay. Let me see if I can find them. And there. Just it was in the same area of the video. But it's. But they can you can see it everywhere. I think you would be able to see it, but most just a small security video in three minutes about how do we handle it. And those are some of my coworkers.

02:33:57  
*Speaker 1:* Let me just this a nonsense.

02:34:00  
*Speaker 2:* They also got the. Elon Musk. I'll click a link on the on scene. There's video we reported on fishing.

02:34:18  
*Speaker 1:* Fishing and form for cyber and for encryption for 9% for trolling. So some caught up and found some data they forgot to score a meal or, in an actual metaphor. The meals in hell of setting a logo up. Some akin to the dolphins for scaly tuber. Fishing here on a spear phishing button. If the persona SEO fraud scare no one person in organization or in the telephone bill Miller by the court or for ping level give to your Palo Alto unit to offer had a violent felony percent dealer fishing maelstrom. Well, to sell a gangster statement for 3% to 10% to 10%. Statistic and post. You first heard that via a data for all these cool 85 million phishing mails and download, because the tailored phishing forces the editing missed and then the increase for organization. But then, she added fishing for soluble in water and meal for service to support. I'll give the password via link. Link still up once in the console, but one intercepted password as gifted noodle one. At our death information center. Hagen server bought a new one and the same password for poor.

02:35:52  
*Speaker 2:* The familiar best practice is our server can be a set of data or fish. The victim of a maximum of open domains of skill is. Here is the angle of persona of Ella Pelham or don't look at link unclear but see all two factor is the bullet or optical software. Link to contact service desk for that. No Talk for artsy boss video. We hope to do a late night. But I don't know when they set Oregon online.

02:36:33  
*Speaker 1:* You can use that one if.

02:36:34  
*Speaker 2:* You.

02:36:34  
*Speaker 1:* Want to, but there's nothing convincing in it. But we made 2 or 3 of those.

02:36:38  
*Speaker 2:* Videos.

02:36:38  
*Speaker 1:* So far.

02:36:39  
*Speaker 2:* It probably is that it makes some, uh, some insert department issue because the security teaching is the information security. And then we start making videos and they got pierced and so on. But I think it's worked out by now. But we've done a few, but we are not allowed to send them out to everyone. So he checked those we can put in the website and say go look. But again we have one hour and that's information security, uh, job. We try to indicate if someone we see something doing something bad will actually they break the law. For example, the one I had right before where they had downloaded the Chinese, uh, office thing, they'll get an email saying, hey, by the way, you're not allowed to own software. We also see people trying to learn VPN software. You can't do that. We have we've hidden all laptops already, so it'll conflict. But we had 49 triangles last month anyway, so we're actually trying to automate and say if you see any download files with the pen name, they'll get an email saying, by the way, you're not allowed to use the software, you're allowed to use approved software. Here's a link to our the rules. And who's that? So you're trying to do some automation about that. So we don't need to talk to people. Just sleep by the way. Don't do it. So that's kind of what we're trying to educate people. But it is not our main focus. That would be information security.

02:38:01  
*Speaker 1:* Yeah. But back to the rubber ducky. Yeah. So as far as I understood that Rubber Ducky is based on the Raspberry Pi software, which softwares are the most popular to get to to produce a tag?

02:38:21  
*Speaker 2:* Uh, and honestly, no clue that they, they do with their own software most of the time. So what they're trying the what they're trying to do, the problem ones is the ones are trying to be legitimate. For example, the Chinese one, we just had to say it's not illegitimate to the proof software. But technically, if anyone open a document, they might lose data. But there was an attack recently. It failed by pure luck. Uh, but someone, uh, most likely Chinese, uh, decided that, hey, there is a specific sub, uh, program for Linux that has whether the one guy on GitHub running this one and keeping up to date, uh, the guy, he had 3 or 4 accounts. The all actually, uh, made various software on GitHub, useful software people to build their credentials. And they spent over three years infiltrating him enough to having some of their useful accounts saying, hey, why don't you update us more often? But as a new update and pushing him and saying, hey, I have some person. It's a free time. Hope you have some problems. I can't just anyway and the manage to push enough to get one of the guy's accounts as a core admin, and then added a small keylogger into this one that was used worldwide. It was only found because in the beta, some weirdo at a company somewhere think Microsoft actually noticed a 0.02 seconds delay when he did something and he deep dived what is happening in front of the actual key login? And that code was legitimate and a legitimate untrusted piece of code. That's where the problem is that if someone can manage to do it in a trusted code, like the backdoor Microsoft NSA had on, that was due to blue key for the mask in two attacks. Holes Holds in proprietary code, like an open source code for that matter is the biggest problem because it's trust code. We actually going down and saying GitHub, we don't really like GitHub that much because it's great, but who owns it? Whatever you do in GitHub, can they change it? Well, a guy recently who is coding himself. His program use escape a lot. Escape is a key that's hard to read when you do the ten finger writing. So we used a little GitHub program to change his escape to his control key. That's great. Problem is, right now you have a weird problem. GitHub is locking which keys you're pressing. That's called a keylogger, and it takes around two lines of code to change the key logging. How much do you trust that guy? Because we don't. So he had children. You're not allowed to do that. He got pissed. But sorry. You installed a potential keylogger against or root host and stop complaining. Because the hacker will do the tools. They'll get code fairly fast, but if they can hide it in something trustworthy, that's. That's a big problem for us. Or again, if some weird medical system are not allowed to update and then we can't even patch the problems.

02:41:32  
*Speaker 1:* I would say, oh.

02:41:34  
*Speaker 2:* Yeah, I hope you got a little paranoid. That's usually the case after I'm done talking.

02:41:40  
*Speaker 1:* Actually, this information was very helpful.

02:41:42  
*Speaker 2:* I was actually wondering how you could use it. You can use it because anyone can learn from this.

02:41:50  
*Speaker 1:* I would say I need to create the rulebook in comparison from Denmark to Ukraine, since I'm working with some IT specialists in Ukraine. So probably I'm going to return to you next time to get an opinion on the strategy that they use.

02:42:05  
*Speaker 2:* You just made me see.

02:42:06  
*Speaker 1:* Yeah, yeah. But thank you a lot for today.

02:42:09  
*Speaker 2:* No problem. Um, if you have interest, um, do you also look into the position?