Interviewer: Can you introduce yourself a little bit?

Expert: I'm an information security consultant here. I've been working with cybersecurity for the last ten years or so. I started as an external consultant in a private consulting company, then I worked in the Ministry of Education for about four years. I started here at in December, so it's been about 4-5 months. The basics of working with cybersecurity remain the same across organizations, but there are differences. In the Ministry of Education, the focus was more on GDPR compliance and protecting data of children and young adults. Here, the work is more on the technical side.

Interviewer: How interconnected is Copenhagen's metro control system with other critical digital infrastructures, and what potential cascading failure scenarios concern you most?

Expert: Let me clarify something first. We are considered critical infrastructure because we're involved with trains. However, our company specifically handles the construction part of the Metro - building the stations, tracks, and similar infrastructure. Our sister company, Metro Service, is the one actually running the trains. They're definitely part of critical infrastructure.

Our ownership structure is 50% state-owned, 25% owned by Copenhagen Municipality, and 25% by Frederiksberg Municipality. These owners are part of critical infrastructure. We've decided that we should align with the related regulations coming into effect this summer, even though we technically aren't classified as critical infrastructure ourselves.

Interviewer: How would you reflect on hybrid warfare in relation to my thesis? I described the healthcare sector, but how would you reflect on the transportation sector?

Expert: We are very aware of hybrid warfare threats. The level of threats and attacks has increased approximately 300% since the Ukraine war began. That's a direct quote from global cybersecurity sources. It might have increased even more in the past six months. We are attacked massively, as is everyone else. This is very high on our agenda - constantly working to push back against these attacks. It's not a question of if you're going to be attacked, it's about when.

Interviewer: In relation to adversaries, which countries are you most concerned about that pose the greatest danger right now?

Expert: Russia, no doubt, and China. I attend many cybersecurity courses, discussion groups, and receive regular updates from different cybersecurity organizations. The general consensus across these forums is that a large part of the attacks can be traced back to Russia. There's no doubt about that.

Interviewer: How would you describe the awareness level of your colleagues who are not related to the IT department regarding cybercrime?

Expert: I was actually surprised when I joined this company four months ago that the awareness level was quite low. My perspective on awareness is that employees are both the greatest

strength and the greatest weakness of any organization - the difference between those two states comes down to awareness.

About a month ago, I introduced a code of conduct - an information security policy written at the employee level. It explains what employees need to be aware of and what they need to do, written in simple, straightforward language.

We're running various awareness campaigns. It's not very academic, but the reality is that we have technical security on one side and human error on the other. Approximately 40% of employees don't lock their computer screens when leaving their workstations - it's equivalent to leaving your home with the front door wide open. Next week, we're launching a campaign where we'll walk through offices during lunch breaks to test which computers are unlocked. Unfortunately, the general level of awareness is low, which is why we're working on it.

Interviewer: Would you say that this is based on cultural factors, since Denmark is a trust-based society?

Expert: Yes. Being a trust-based society is actually positive, and being one of the most digitalized countries is good too. But when you combine these two factors in the context of cybercrime, it creates significant vulnerabilities. As you noted in your thesis, we are vulnerable as a country. Most people appreciate our high level of digitalization and our trustworthy, polite culture, but they don't connect these characteristics to cybersecurity implications - and that's the issue.

Interviewer: How would you reflect on the legacy systems in your company? For example, do you use any old, outdated systems to run some processes?

Expert: No, actually not, because we're quite a young company - only 23 years old. We started around 2000, so our systems are relatively young. As far as I know, we don't have any legacy systems.

Interviewer: What physical-digital security intersections present the most complex challenges in metro security management?

Expert: I need to clarify that I can only speak about Metro Copenhagen - the construction company where I work - not Metro Service, which runs the trains.

I think the main issue is that our maturity level is low. We have Microsoft 365 Defender, which is a very advanced system to protect us. We paid a lot of money for it, but nobody had properly installed it to ensure it works effectively. When I discovered this, I realized we needed to bring in specialists to set it up properly.

Looking at security standards, at the top of the pyramid you have policies - the "why" of cybersecurity. The next level is ISO 27001, which addresses who's going to implement security measures. Then there's AT-18 compliance, which details how to implement security at a concrete, technical level. Nobody in this company was knowledgeable about these frameworks,

so we're bringing in external experts to assess our current level and develop a roadmap for improvement. This will take 1-2 years.

Part of the challenge is that we have sophisticated tools like Microsoft 365 Defender, but no one knew how to use them effectively to prevent cyber attacks. It's a journey we're on, and we'll likely reach our goals in 2-3 years. This comes down to investment decisions - balancing costs and benefits - and resource constraints. There's a shortage of qualified cybersecurity professionals, so we have to make careful decisions about resource allocation.

Interviewer: How would you describe the political influence on Metro security and the transportation sector's security as a whole?

Expert: New regulations are coming up that place responsibility directly on the board of directors. When board members have personal liability, it changes their perspective significantly. We're having a board meeting in 2-3 weeks with our new chairman, Tom Atlas, who is very aware of these new regulations and their implications for our company and the board members. There's definitely awareness at that level.

Interviewer: In my thesis, I described that some public companies lack a centralized system of command. Based on my findings, would you suggest improvements to your company's structure, particularly regarding who to contact when security issues arise?

Expert: That's a very good question. We're working on that right now. We have an incident response plan that outlines who does what and when if an incident occurs. The existing plan wasn't very good, so I've rewritten it. We're planning to conduct a tabletop exercise where we'll run through different scenarios to test the plan and then refine it based on what we learn.

Just this morning, we had a meeting about creating a "war room" for handling incidents. This includes having standalone computers, backup batteries, and specific software ready for emergency situations. This hasn't existed in the company before, but it will be established within the next two weeks. As I mentioned, the security maturity level of this company is quite low, and I'm working to increase it.

Interviewer: My thesis discusses current problems with digitalization. If you were the IT security chief of the entire department, how would these issues affect your thinking about the company?

Expert: We're already at a very high digital level, so the question is whether increasing digitalization further would be beneficial.

Interviewer: What would be the trade-off between digitalization and passenger convenience? As I understand, the metros don't have drivers and are fully operated by automated systems. How do you secure passenger safety given developments in AI and quantum computing, where a hacker infiltrating your systems could put passengers' lives at risk?

Expert: There's always a trade-off. The system could be completely manual with drivers operating the trains, but even then, the signaling systems telling trains when to stop and go could be hacked. It's a question of efficiency and cost - human operators cost money, while technology, though expensive initially, is much faster and more efficient.

When you're running metro trains that arrive every two minutes, manual control becomes difficult because it's simply not fast enough. Right now, some of our tracks are running at over 100% capacity. If we moved to a more manual system, capacity would drop significantly, which would require building additional tracks - a multi-billion investment that's not feasible.

The high-tech approach does make us vulnerable, particularly with quantum computing potentially becoming reality in the next 5-10 years. We're very aware of this risk, and there are many security measures built into our systems.

We also plan for contingencies like major power outages or flooding in underground sections. There are multiple safety mechanisms in place. For example, if there's an emergency, trains are programmed to continue to the nearest platform to evacuate passengers. If the system or electricity is down for more than about 15 minutes, all doors open automatically and people must walk through the tunnels to reach stations. Before restarting operations, metro workers have to inspect the entire system to ensure no passengers remain on the tracks, which can take 1-2 hours.

As a failsafe, the trains can be operated manually. There's a control panel in the front of each train that can be used for manual operation if necessary.

Interviewer: I noticed that some panels on top of the metro cars had fallen off, revealing interconnected cords. How would this affect the threat level if someone decided to tamper with those components?

Expert: That's certainly a possibility, though I'm not sure I'd classify it strictly as a cyber risk - it's more of a physical tampering risk. People can cut cables or place objects on tracks, which would certainly cause problems. As I mentioned earlier, the trains are programmed to respond to emergencies by proceeding to the nearest platform when possible. If power is lost for more than about 15 minutes, the doors will open automatically to allow evacuation.

Interviewer: Have you read about the recent incident this week where some European countries were left without electricity? How would you compare the potential impact of a similar situation in Denmark?

Expert: It would cause complete chaos due to our high level of digitalization. All our phones would die. My Tesla - I couldn't even open the door without electricity on my phone, and I couldn't drive further because my "gasoline" is electricity. I don't even carry a physical credit card anymore - I only use my phone for payments, so I wouldn't be able to pay for anything. Denmark's high digitalization level makes us very vulnerable to electricity disruptions.

Interviewer: How would you say we're dependent on collaboration with external countries? You mentioned using Microsoft-based solutions to monitor security risks. How has the development of US politics toward Denmark affected security understanding overall?

Expert: It has definitely had an impact. As you noted in your thesis, approximately 90% of global data is stored in the US, which is problematic. In cybersecurity discussion groups, there's growing concern about developments in the US. We're talking about Amazon with all their data centers, and Microsoft Office, which is used by over 90% of both private and public offices. If these systems were somehow blocked or compromised by US actions, it would create major problems for our email systems, productivity software, and more.

There's a growing level of concern about how to proceed, as US-based software companies aren't perceived as reliable as they once were. I believe there will be increasing European interest in establishing data centers controlled by European countries. The political situation in the US has definitely raised awareness about how dependent we are on American companies.

Looking forward, I expect more focus on hosting both software systems and data centers in Europe. This won't happen overnight because it requires massive investment in software development and physical infrastructure, but I think we'll see a shift over the next 4-6 years, with Europe moving to store data within its own borders under European control. The political developments in the US have served as a wake-up call for many who weren't previously concerned about these dependencies.

Interviewer: How did my thesis affect your thinking? Did it support hypotheses you already had, or did it bring new knowledge?

Expert: I found your angle on Ukraine particularly interesting - how Ukraine has been targeted most heavily by Russian cyberattacks, and the lessons that can be learned from their experience and applied to the rest of Europe. I hadn't thought about it from that perspective before.

It's similar to what's happening on the military front - Denmark is now sending military personnel to Ukraine to learn about drone technology, where Ukraine has developed world-leading capabilities through necessity. The rest of Europe and the world can learn from what Ukraine has built. When I read your thesis, I saw the parallel with Danish soldiers going to Ukraine to learn about drone technology - it follows the same pattern of knowledge transfer. That's a very interesting perspective.

Interviewer: What recommendations would you give on supplementing the theories I presented, for example, regarding political tensions between countries and the vulnerability of cyberspace?

Expert: The main priority for Europe should be moving software capabilities and data centers to European territory to create a more stable and independent system. Denmark, as highly digitalized as it is, is by definition vulnerable.

There's always a cost-benefit trade-off. If you want to run a metro company extremely efficiently, it has to operate at a very high technical level, which introduces vulnerabilities. On the other hand, using lower-tech approaches reduces efficiency.

Denmark is one of the wealthiest countries in the world despite having limited natural resources. This prosperity is largely due to high efficiency achieved through digitalization. My daughter, who's a bit younger than you, is currently in France and is amazed at their low level of digitalization. What might require multiple forms, stamps, and visits to offices in France can be done with five clicks on a mobile phone in Denmark. That's one of the reasons Denmark is so wealthy - because of the high level of technology adoption.

Interviewer: Does the introduction of new apps into current systems bring you comfort, or does it also raise concerns?

Expert: It's always a trade-off between efficiency and security. That balance is constantly being evaluated.

Interviewer: Does it concern you that, as I mentioned in my thesis, some people can reverse engineer apps? For example, students from my university reverse engineered certain transit apps and found backdoors that could be used to enumerate users and potentially compromise private information. Does this make you uncomfortable about digitalization?

Expert: Not really, because I'm already aware of these risks. That's the interesting part of working in security - the technology is constantly evolving, laws are changing all the time, and hacker techniques are continuously advancing. That's why, even though I'm approaching 60, cybersecurity remains fascinating - it's always changing.

I hope you and others with your skills will find cybersecurity extremely interesting because the development never ends. Our job in cybersecurity is trying to stay just a little ahead of the hackers. We don't always succeed, but that's what we strive for.

Interviewer: What recommendations would you have for the upcoming generation of cybersecurity specialists based on what you've read and experienced yourself?

Expert: First of all, you're in a very comfortable situation because there's a massive shortage of cybersecurity professionals. You have job security and can expect high salary levels - so congratulations! We're always discussing the fact that there are far too few specialists with cybersecurity skills.

On a practical level, you could work as an external consultant educating both private and public companies - that's one career path. You can also work in public organizations like ministries or in private companies like this one. My recommendation is to try all of these options because you'll gain different perspectives and develop different skills.

I originally trained as an economist and worked in financial planning for about 25-28 years before changing my career path when I turned 50. I'm 60 now, and the last ten years have been incredible. So definitely jump in and try different career paths in both public and private sectors.

Interviewer: I don't have any more questions.