Expert: My name is “Expert” and I've been working at this “Hospital A”since 2002, giving me a long history of what's actually happening here. I've held many different responsibilities throughout my tenure. In 2009, they outsourced my primary responsibilities and essentially restricted me from leaving the building. When I asked what I could do instead, I was assigned to antivirus management—mainly because no one cared about it at the time.

For years, security was neglected. There was no dedicated security department whatsoever. “Hospital A” had no interest in IT security at the enterprise level. My coworker and I could barely keep things functioning, let alone improve them. During department meetings, we consistently informed leadership not to worry about any SLA agreements on security cases because we simply couldn't handle the volume.

Four years ago, we finally established a proper security department, starting with me and my colleague. Today, we've grown to 26 people, which is unprecedented growth for a public service department. Despite this expansion, we still have just as much work because our scope has expanded from just enterprise-level concerns to everything security-related. Now we actually have time to investigate problems, and every time we touch anything, we discover more issues that need addressing.

The main challenge for hospitals is legacy software—and we have plenty of it. While we've closed the last Windows 2000 systems last year, we still maintain Windows XP, Windows 7, and other outdated systems. The problem becomes more complex with medical devices because these are physical systems with limited suppliers.

We can't always dictate security requirements because when there are only one or two suppliers worldwide, our leverage is limited. Sometimes we face difficult choices between implementing proper security measures or ensuring patient care continues uninterrupted.

For example—without naming the specific department—we have an issue where there's unrestricted access to patient data through general user accounts, which is a GDPR concern. The only immediate fix would be to close the network shares, but doing so would halt critical treatment for approximately 120 patients. The alternative solution is to implement new software, but that requires an EU tender process which takes up to a year and a half.

In such cases, our information security team documents the exception, explains why we can't immediately address the issue, and outlines our mitigation plan and timeline. This approach helps us avoid GDPR fines while we work toward a proper solution. We're much more mature in our documentation processes now, which is a significant improvement.

We've made substantial progress in controlling unauthorized software deployments. Previously, departments would purchase and install whatever they wanted without consulting IT. The "ask for forgiveness rather than permission" approach was widespread. We've significantly reduced this practice by establishing consequences—if departments purchase software that doesn't meet our security requirements, it gets removed. People are learning, though we still have a long way to go.

The challenge remains with specialized medical software. For instance, we have a major patient system that doesn't run our antivirus because it operates at such a micro level that the antivirus interferes with its functioning. We lost that particular battle because there are only two suppliers worldwide for this system, and neither would accommodate our antivirus requirements. Sometimes we simply can't win these conflicts when the medical necessity outweighs the security concerns.

The "we'll do it tomorrow" attitude that's been normal in public service for years is finally changing. My new boss was specifically hired to be persistent and push for action, and it's working. It took about a year and a half for the organization to realize that when my team raises security concerns, they're genuinely important and won't just disappear if ignored. We've established an effective escalation path—if departments ignore our recommendations, we escalate to their managers, which has proven effective.

This approach has even influenced other infrastructure managers to expect results and hold their teams accountable, improving the organization as a whole.

Our ongoing challenges remain legacy software and user behavior—users are always the weakest link in security. In our hospital environment, we must maintain flexibility because there's a legitimate use case for almost everything. We always have exceptions to whatever rules we create.

For example, we blocked a service provider after experiencing 20 phishing attacks from their platform, where anyone with an email could create a website. However, we had to make an exception for one user because their department had purchased a small website on that platform that couldn't be accessed otherwise.

Another example involves content filtering. In most organizations, pornographic content would be universally blocked. However, we have plastic surgeons, psychologists, and psychiatric ward staff who legitimately need access to content that would typically be restricted. Some psychiatric patients would require medication or restraint if staff couldn't access certain materials for therapeutic purposes.

Our general policy for employees is that as long as they don't install unauthorized software or break the law, how they use their time is between them and their manager, not the IT department. We might provide activity logs to managers upon request, but we don't proactively police general internet usage.

Despite our generally permissive approach, we have blocked a few websites for security reasons:

1. TikTok and Snapchat were blocked because people were sharing GDPR-protected information on these platforms.
2. Teams Web was blocked because its permissions requirements were excessive, essentially allowing access to everything on users' phones, including the ability to take devices out of sleep mode, record activities, and transmit that data.

3. During the COVID pandemic, we blocked a website created by vaccine skeptics that allowed users to generate fake COVID-19 vaccination certificates.

We're improving our security posture by implementing machine isolation. In the past, if a user downloaded malicious software or compromised their machine, we might eventually notice it, attempt to contact them, and resolve the issue—a process that could take hours or days, especially since many users don't have current contact information in our system.

Now we're working on automated isolation capabilities. If a user does something suspicious, their machine is automatically isolated from the network. They can't access anything, while we can still remotely access their machine to investigate the issue. This allows us to be proactive and address security incidents before they escalate, rather than just relying on our monitoring systems to detect problems after the fact.

Expert: 95% of malware comes through emails. That's been our main risk since I started doing these presentations in 2017. The percentage hasn't changed. Similarly, one out of 13 web connections leads to a malware site. This has also remained constant since 2017.

Expert: Before recent geopolitical events, I mainly focused on money as the primary motivation, but there are four main reasons people attack systems:

1. **Money** - Simple financial gain from malware
    - For example, North Korea trying to get cash
    - Financial incentives in different countries can be significant (e.g., $8,000/year for software development in Romania vs. $100,000 elsewhere)
    - Countries with weak rule of law make prosecution difficult
2. **Ideology** - Nation states or organized groups with political goals
    - Russia, North Korea, and others use cyber attacks for ideological purposes
3. **Compromise** - Insider threats stealing data
    - Both intentional and accidental breaches occur
    - Example: Japanese employee who was fired after losing a USB stick with 4.2 million citizens' data
    - Example: Denmark accidentally sending 4.5 million CPR numbers to the Chinese embassy
4. **Ego** - Often from former employees with grudges

Expert: The cybersecurity network on the darknet is quite advanced. With about $2,000-$3,000, you can buy ransomware attack software complete with 24/7 support. They even offer video support and 24-hour service level agreements for creating new versions that won't be caught by antivirus software. Their support is better than ours.

These criminals are often untouchable in Eastern Europe because they either work for the government or can bribe police. However, a few years ago, three major cybercriminal bosses were caught when they traveled to London or New York.

Expert: About a month ago, a Russian propaganda agency had almost all their internal documentation leaked. Russia has been involved in propaganda and election manipulation for years, but has denied it. This leak revealed they had 20 meetings with Western governments and bragged about successful election interference in Germany and France.

One example was creating a false story about Ukraine harvesting organs, which was shared by Marjorie Taylor Greene, a Trump supporter in the US. This shows how governments try to affect public opinion.

Expert: After recent events in Israel, there are concerns about sabotage through technology. The New York Times reported Israel was involved in operations involving booby-trapped devices. This raises serious security concerns:

- Can Apple guarantee what happened to your MacBook before you got it? No.
- Can our suppliers guarantee there's no explosive device? No.
- What do we do if spy agencies create fake companies and produce hardware themselves?

This isn't just Israel. The US NSA intercepted Cisco hardware in transit for years, adding surveillance packages and resealing devices to look untampered with. This was leaked by Snowden.

Another example is Stuxnet, created by Israel and the US to destroy Iran's nuclear centrifuges. While it worked, 59% of the damage was in Iran, but the rest affected systems worldwide. This shows state actors conducting attacks that can impact unintended targets.

Expert: Emails remain the primary attack vector. Examples include:

- Messages claiming to fix mailbox size issues
- Compromised banner advertisements on news sites

Expert: I used to worry about porn sites back in 2002. Hospital porters would access porn sites during night shifts, triggering malware. We had to reinstall PCs monthly.

Today, mainstream porn sites like Pornhub have strong security because they have financial resources. I'm more concerned about:

- Extra/niche sites with less security funding
- Government websites (every Western government has had at least one site hacked in the last year)
- Trusted sites that get compromised

Expert: In a US survey, when USB sticks were dropped in parking lots, 34-45% of them were actually plugged in and activated. We've seen successful attacks in Denmark using this method. If I dropped 20 USB sticks labeled "Salary Negotiations" in a parking lot, there's a 50% chance someone would plug one in.

Expert: One example is the DDE vulnerability in Microsoft Office. Although DDE hadn't been used since around 2000, Russian hackers discovered it was still functional. After just two clicks in a Word document, they could gain full access to machines.

I created my own test version that appeared to be security-approved documentation asking users to "click yes on the popups." When clicked, it executed commands that could control the user's machine. Microsoft initially didn't want to fix it since it was "as intended," but changed their mind 14 days later.

Expert: Sites like Pirate Bay have used visitors' CPUs for Bitcoin mining at 100% usage while on the website. This is legal if disclosed, but becomes illegal when implemented covertly. These scripts can even physically damage devices - security researchers let one run at 100% CPU power for two days on a phone, and it caused physical damage to the battery.

Expert: In 2013, the NSA had a backdoor to Windows that was stolen. In 2016, a group called Shadow Brokers obtained these tools and put them up for auction. In January 2017, Microsoft identified the problem and, for the first time ever, dropped their regular Patch Tuesday schedule to issue an emergency patch in February.

In May 2017, the WannaCry ransomware attack began, taking down 60% of the UK healthcare system for 14 days. The National Guard had to help reinstall PCs. Microsoft even released a patch for Windows XP, which was no longer supported - something they had never done before.

At our organization, we had to patch all servers that weekend regardless of the consequences. Normally, we're cautious about restarting servers because they might be running critical care systems, but in this case, we had no choice.

Expert: Security researchers found 20 security holes in the TCP/IP stack from 1989, affecting many companies including NASA and Lockheed Martin. The worst part is that many affected organizations don't know they're vulnerable, and these issues still aren't fixed. Potentially every IoT device in the world could be affected.

Expert: We see many phishing attempts. One example was an email that appeared to be from users to themselves with a text file attachment. 19 people clicked on it in one week.

When I followed up with one user, they said, "That's not my responsibility. I'm not paid to think." This type of attitude is dangerous. Others thought it might be from a printer or for a shared mailbox, which shows they were at least attempting to rationalize.

Expert: Sometimes legitimate organizations make serious security mistakes. A Danish library sent emails asking users to send scans of their Danish health insurance cards, passports, or driving licenses to an unencrypted email address. This violated privacy laws in at least four different ways.

We also deal with a Saudi Arabian health insurance company that covers embassies in the Middle East. They regularly send unencrypted patient information and don't care about GDPR

violations. We remove all patient information when we reply to avoid breaking the law ourselves.

Expert: We've seen sophisticated phishing attempts. One included a user's actual password from a LinkedIn breach to make the scam more credible. LinkedIn lost 164 million email addresses and passwords in 2012, and this dataset was sold four years later, allowing scammers to use real passwords in their blackmail attempts.

I recommend everyone use the "Have I Been Pwned" website to check if their email has been compromised in any breaches. Companies can also sign up for notifications.

Expert: Data breaches can have serious consequences:

- Adult dating sites like AdultFriendFinder lost 4 million records including personal information
- Ashley Madison, a site for extramarital affairs, lost 30 million accounts including payment details and physical addresses, leading to some users committing suicide
- Even more sensitive sites like bestiality forums have been breached, affecting people who would be extremely motivated to pay blackmail

Expert: Business email compromise is increasing in sophistication. One example targeted one of our middle managers with a perfectly written email - the only mistake was using the wrong company logo.

These days, scammers often first request iTunes gift cards rather than bank transfers because gift cards can't be reversed. In the last two years, we know of at least two cases where “Hospital A” employees sent gift cards worth 2,500 kroner.

Interviewer: I know the monthly average income in Ukraine is around 1,000 to 2,000 Danish kroner.

Expert: Exactly, which makes these scams very profitable for attackers in certain countries.

Expert: We had a situation where it was a monthly payment scam. People fall for it when told their yearly income verification is complete. Sadly, when people get caught in these scams, I try to spend about five minutes explaining what happened. Nowadays, if someone asks for money, you should meet them physically—not via email or phone—and get it properly approved.

The consequences can be severe. One of the big museums lost over 800,000 kroner in half a year because they used to approve large art purchases remotely. In 2022, there was a significant change in Denmark regarding loans. Out of 40.5 million kroner in loans, scammers extracted 21.9 million. Some victims have even committed suicide after losing their life savings.

As a man, I receive messages at least once a month from "attractive women in swimsuits" wanting my credit card details on Facebook. That's unfortunately common.

Interviewer: I have a Facebook account, but I don't really use it.

Expert: You'll probably get similar invitations about once a month, usually from people in military uniforms or suits who would "love to meet you." Is your Facebook registered in Ukraine or Denmark? That actually matters.

Interviewer: I think in Denmark.

Expert: That explains it. My wife is from the Philippines, and she never received scam attempts while living there because the Philippines is a poorer country. There's no profit in scamming people who don't have money. As soon as she moved to Denmark, she started receiving scam attempts. Scammers know where the money is.

The good news is that in 2023, reported scam losses in Denmark decreased to 17 million kroner. But that's still a lot of money and represents many people's life savings. Despite numerous news stories about these scams, people continue to fall for them.

Expert: Deepfakes present another serious concern. Taylor Swift recently had deepfakes of herself and a football team created in pornographic contexts. This issue has even been addressed in the U.S. Congress, but there's not much that can be done. It's already illegal, but enforcement is difficult.

A 2019 study by a Detroit security company found that 96% of online deepfake videos were non-consensual pornography. This affects celebrities, ex-partners, stalking victims—anyone can become a target. Women are more frequently targeted than men.

At our organization, we've had cases where people have been stalked, and we try to help. We've also had cases where people believed they were being stalked but weren't. These cases are challenging to handle. I'm good with people, unlike some of my colleagues who are very black-and-white in their approach. The problem is that as IT departments, we can't tell someone they need psychiatric help—we can only talk to their supervisors.

In one case, a supervisor recognized an employee's problem and helped them get assistance, which led to improvement. In another case, an employee was fired because she was spending five hours a day being paranoid and couldn't perform her job.

Expert: Deepfakes can also be used for sophisticated financial fraud. A company in the UK lost £25 million in February due to such a scam. The fraudsters exploited cultural differences—in Asia, there's a tendency to not question superiors. This wouldn't work as effectively in Denmark, where employees are more likely to question unusual requests from management.

The scammers set up a fake board meeting, filmed from a distance to be convincing but not close enough to reveal the deception. They created an entire one-hour fake board meeting. During this meeting, the chief economic officer was instructed to make six transfers totaling $24 million, which he did because that aligned with cultural expectations in that context.

This is why we now require physical meetings for money transfers. Currently, technology exists that combines real-time deepfakes with AI like ChatGPT, which can speak Danish. When you reply, it can generate video responses and maintain a conversation. This has already been demonstrated and will only become more sophisticated. I worry because while we can train people to identify fake emails, it's much harder to recognize a fake video call that appears to be from your boss requesting a money transfer.

Expert: There's also significant misuse of legal systems. In a recent case, a couple went to Disneyland in the U.S. and ate at a restaurant where they informed staff about a peanut allergy. The restaurant made a mistake and served food containing peanuts, resulting in a fatality. The surviving partner sued for $50,000, which is relatively modest in the U.S. legal system.

Disney, instead of directing the lawsuit to the restaurant operator who rented the space, attempted to claim that by signing up for their services, customers waive their right to sue Disney for any reason, including poisoning. Disney eventually withdrew this position due to backlash.

Uber has been similarly problematic. A couple who used Uber were involved in an accident and sustained significant injuries. When they tried to sue, Uber's lawyers convinced a judge that because the latest app update included a waiver of the right to trial by jury in case of accidents, the lawsuit couldn't proceed. This is concerning because most users don't read these terms and conditions.

Expert: We had a case some years ago at a hospital involving an intensive care surveillance unit with nine computers monitoring intensive care beds and one central computer displaying all nine beds' data for 24/7 staff observation. When this surveillance system lost internet access, it incorrectly showed "heart failure" for all beds in the intensive care unit.

Fortunately, the patients weren't actually experiencing heart failure, but staff had to physically check each patient. In the worst case, this could have caused deaths. The vendor's response was dismissive: "We don't care. It's supposed to work like that." We barred one of their employees from approaching any hospital for six months after that incident.

Expert: Foreign state actors, such as Russia, have successfully hacked our defense systems. Russia officially denies state-sponsored hacking, which is technically true—the Russian government itself doesn't engage in computer hacking. Instead, they have groups doing it on their behalf.

How did they breach our systems? They sent a phishing email requesting login credentials for an unclassified web-based mail system. This gave them access to Danish defense systems for two years.

The UK's National Health Service experienced a similar attack that affected 60% of UK hospitals for 40 days. The official cost was reported as £180,000, which seemed suspiciously low. Last year, a better estimate put the cost at £92 million, which is probably still too low.

Expert: Maersk suffered a major attack that officially cost them $2 billion. The interesting part is that they weren't even the intended target—this was collateral damage. A group of Russian-speaking hackers targeted Ukraine by exploiting a specific economic program that Ukrainian businesses are required to use for government interactions.

The hackers installed a backdoor in the latest version of this software, which affected companies worldwide, including Maersk. The attack completely disabled Maersk's systems—they had no idea where any of their containers were or what was in them. The only reason Maersk survived as a company was pure luck: they had one Active Directory server in South Africa that was offline for maintenance at the time of the attack. If that server had been online, the company might have collapsed entirely.

This incident actually helped increase cybersecurity awareness in Denmark. We saw a significant increase in people calling our services to verify suspicious emails. Whenever I meet a Maersk employee who was there during the attack, I thank them because "they took one for the team" by raising awareness.

Expert: About 94% of attacks come through email. We receive approximately 6.8 million emails per month: 4.5 million are clean, 1.9 million are spam, and 3,000 contain malicious files. Sometimes malicious emails get through our filters, and people click on them without thinking.

Expert: Physical security is equally important. When you received your access card downstairs, you probably noticed our protocols. People often don't think and will let others in when they hear someone at the door. If I don't know the person, I need to check their credentials before allowing entry. Some people get upset about this, but it's necessary—we've had security breaches.

In one case, an unauthorized person walked in, went up to the third floor, entered our boss's office, and stole a phone from the service desk. We have video evidence but couldn't identify him. He tried to return a month later, but we recognized him and removed him. He tried again, and we removed him again. We haven't seen him since.

When you're issued an access card here, you receive a PIN code on the back of the card. In the past, approximately 20% of building occupants would keep their PIN code on a post-it note attached to their card—if someone found the dropped card, they would have full access under that person's name.

Interviewer: Would that happen with this card?

Expert: You probably won't have that issue with this card specifically because you need to pass through our security desk. However, we can't completely restrict access to hospitals because patients need access to most areas. We can't close off intensive care or emergency units just for security reasons, though I'd prefer to if possible.

Expert: Improper security can lead to significant fines. Midtjylland received a 400,000 kroner fine and police investigation for a serious breach a few years ago. They gave every employee and patient access to a building containing approximately 100,000 physical patient journals with

personal information and identification numbers. Everyone had keycard access to everything in the building regardless of their role, including patients. That's a suicide move from a security perspective.

Expert: From a leak of 3.4 million PIN codes, we discovered that the top ten most common PINs account for nearly 24% of all four-digit codes. This is particularly problematic for securing areas with PIN-based padlocks.

We use a company for the destruction of sensitive materials. I once needed to print documents for my wife's nursing education, and I accidentally placed them in the secure disposal bin. How long do you think it took me to access that bin?

Interviewer: A day?

Expert: Ten seconds. The code was set to 1-1-2-3, so I tried 0-1-2-3, and it worked. I then checked other bins in the building and discovered they all used the same code, giving me access to our entire organization's confidential waste. This included materials from the team responsible for our contract with the disposal company. I reported this three times before anything happened. Our lawyers finally intervened, and they changed the code.

What's especially concerning is that when my wife, who is from the Philippines, needed to renew her residency permit, we visited the immigration office. While waiting, I noticed their disposal bins and successfully guessed the same PIN code. This means I could potentially access sensitive documents from numerous government agencies just by wearing a janitor's uniform and claiming I need to access the bins.

People simply don't think about security. When we hire new staff, we take them through the hospital to show them how it operates. An adversary wouldn't necessarily need to hack through firewalls—someone with physical access could place a small device to capture data. The delivery areas are particularly vulnerable, with minimal surveillance and potentially interesting shipments secured by simple four-digit codes.

Expert: Let's talk about physical security. There's no way to stop me because no one knows what this is for. It happens everywhere - from full access for cars to expensive medications. If you want them, go to all places with Bluetooth devices. It doesn't matter - we are really bad at physical security.

The Internet of Things is a major problem because everything needs to be online today. What can you hack? Do you have antivirus on your IoT devices at home? No, you don't.

Toothbrushes are online. Why? When I started this presentation, toothbrushes were not online - they were just Bluetooth connected. You could buy a small ruler with a suction cup so you could put your phone on the mirror in your bathroom to record your toothbrush in real time and get feedback on how you're doing. That's apparently a great argument for having a toothbrush online. You can also get achievements and compare your brushing with others. Perfect! And of course, you can also hack it.

There was an article about a potential DDoS attack from toothbrushes. It was theoretical - a German security researcher talked about how it's possible, but someone mistranslated and wrote an article claiming it had happened. It's theoretically possible, they just thought it had actually occurred.

How about a box to keep eggs in? It's on Amazon. You can see how many eggs you actually have and how long they've been there, so you know if they're going bad. Perfect.

Why do you need an online fork? The idea is that people my size eat too fast, and this fork can vibrate when we eat too fast. You can upload what you're eating, what you're making, the calorie count, and so on. That business closed now.

If you had $100 you didn't know what to use for, you could buy an online toilet. I've been waiting for that for some years. I could only find Bluetooth-connected toilets in English, though you can get them in Japan. Now they're finally here, so you can spend $1,870 on that toilet!

We do have some online toilets for medical purposes - for example, for dialysis. If you need to measure a patient's fluid intake and output, it's easier to have them use a smart toilet than pee in a cup. So it's actually a good idea for medical use, but for home use, I don't see why I need a toilet with an app to control everything.

In the future, they expect around 20.6 billion IoT devices a year. By 2025, the value of the subscription market will be $58 billion. For cybersecurity, they expect there will be 3.5 million security workers in 2025. In 2021, the number was still 3.5 million. That hasn't changed despite new indications about security needs in Denmark. It would require massive upskilling of security people, but we haven't changed the number - we've just managed to stay skeptical.

Worst of all, they expected there to be 3.9 trillion IoT devices online. I mentioned 20.9 billion earlier, but with trillions of devices, we don't know how many are hacked.

When I started this conversation, only three of these things were online. Now your smoke detectors, alarm systems, temperature controls, and doors are online. You have Hue bulbs in your home. You can get online toasters - I got one last year. You have coffee machines, dishwashers, and microwaves online. My fridge can be online, though I haven't connected it.

Your car keys are online. Your Roomba - the robot vacuum cleaner - is online. Do you have one?

Interviewer: No.

Expert: Good idea! Because do you know what that is? It's a vacuum cleaner with a camera on wheels. What can I use a camera on wheels for? Two things. I could see if I could get pictures of people inside after they go off the path. I can also use it to scout if they have anything valuable before I break in. And now you give them a camera on wheels that you can hack. Perfect!

Trash cans are now online too. I haven't found an online trash can in Denmark, but I've found trash compactors in the US. In Denmark, we're using connected technology on big public trash cans to see when they're full.

The only thing I can't find online yet is a broom. I can find a broom with little heads that can reach out wirelessly, but I can't find one fully online yet. I'm sure it'll come. It's scary that since 2017, all of these devices have gone online.

This is what I tell people to do:

- Update your software. Patching is the most important thing of all.
- Use a password database. Never reuse passwords. If one site is compromised and you only use one password, hackers have your email and your entire digital history and access.
- Use two-factor authentication
- Back up everything. I've lost nine hard drives in my time in IT with data. Backup means having at least two copies, and hopefully also one outside your home. If you have a break-in or fire, they can steal all your stuff.
    - I have a backup in the cloud
    - My colleague doesn't trust clouds; he has a bank box with a USB disk. Each month he fills it with data and puts it back in the bank. It's cumbersome, but it works.
- Have antivirus to check because if you don't know you're compromised, you can't do anything.
- Think about what you post online. Have you tried Googling your name? It's interesting.

Interviewer: Yeah, I don't think I have anything on my name.

Expert: Who knows? In my case, I've done some translating on comics, which means most of my hits are on LinkedIn or on library sites or book trading sites.

I have a Gmail account. The problem is five other people in the same country have the same name, so once in a while I get their emails. It's all from football teams, new shirts, vacations in Australia, or bills.

One of the things I got was an email from a Danish charity organization. They sent me an email about people joining their weekend event, and they put 97 people in CC. If a company does that, they could get a fine if someone complains to authorities. If it's a charity, it's technically legal, but still a very bad idea.

I emailed them and said, "This is not good. If I was a right-wing idiot, I could probably use those 97 emails to do some damage." A month later, I got another email. I emailed them again. Another month later, same thing.

Then I got frustrated. I spent 20 minutes looking up the people in the emails. I had their email addresses and first names. Twenty minutes later I sent them a message saying, "Here's where you

work. Here are your Facebook profiles. Here's where you live. Here's when you're on vacation. Here's when to break in." That's what I found in 20 minutes! They finally got the message.

It doesn't take much time because people leave a digital footprint that can be used for scams. If I have your email and phone number, I can spoof them. If I know you have a 16-year-old kid, I can send a message: "Hey dad, I broke my iPhone. I need some money for a new phone." This scam works - my coworker recently received one, though he was surprised since he doesn't have kids. The more data I can find on you first, the better, because I can use it.

Patching is the most important thing you can do. If you don't patch, they will get in. Our problem is our size and our leadership because it's hard to patch when they need 24/7 support.

We know that if we try to isolate systems, even Windows XP for example, we can put them behind their own firewall or in their own area not accessible from anywhere else. We have around 40 XP machines isolated this way. We also have people who say, "Hey, can you get a machine to run this because the software doesn't work on anything new." The psychiatric software they use is proprietary, so no one else can make it, and we can't even make our own. We will try to isolate everything we can.

Sometimes we have to make compromises because if we can't send bills to doctors, that's not good. But we can limit the damage by saying at least only specific IP addresses can access it. We've blocked a lot of the world - Ukraine, Russia, China, India, and around 17 or 18 other countries. We open access if people need it for specific sites. For example, someone in Ukraine needed access to RedCap to do some work, and we opened that specific IP address, not the whole country.

We're trying to limit who can access our systems, and yes, we are occasionally frustrating people. We were afraid there would be huge complaints when we blocked the first 12 countries, but we've only had to open access for around 70 unique websites in two years. That's not a problem. And yes, it might inconvenience a doctor, but overall security is more important.

In our firewalls, when someone tries to attack us, we drop the traffic. When we blocked those 12 countries, our dropped traffic decreased by 70%. We didn't expect that much improvement, but it actually gave our firewall a lot of extra capacity because it spent less time dropping traffic from certain countries. This is a big win. That's usually what I use when people complain about why we're blocking India - it's actually a massive attack vector. Of course, if Russia attacked us, they wouldn't do it from Russian IP addresses, but if you can stop 70% of random scripted attacks, you win a lot because sometimes they get lucky.

My department receives emails from the Center for Cybersecurity, CSIS (a security company in Copenhagen), other institutions, SOC units, and a few other sources about any breaches or CVEs they learn about.

Whenever there's a breach, they assign a CVE number saying there's a problem. Today we got a mail about a specific vulnerability where someone found a problem with the Cyber Panel. The

CVE is a security breach number. Big companies like Microsoft will get thousands of these numbers each year. Smaller companies get fewer.

These vulnerabilities are rated from 1 to 10. If it's 8.8 or higher, it's a "patch now" situation where we immediately need to address it. Then we talk to our Windows team or the sponsors of specific systems. For example, I would ask the RedCap team about a RedCap vulnerability before going to ask about a specific subpart of RedCap. If they don't have that component, we don't need to patch.

During the last Patch Tuesday, we had a vulnerability manager who handled all these cases. I looked at all Microsoft issues and found 12 I needed to discuss, with five related to specific software. I asked, "Do you have that installed?" They said no, so we didn't care about those. We ended up needing to patch just one issue on some zip servers, out of a few hundred potential vulnerabilities, because the rest were low priority and could wait for normal patching.

Anything important we try to patch right away if possible. There will be cases where we can't do it. If there's a 24/7 system for intensive care, we might need to warn them and coordinate carefully. But patching is probably the biggest and most important part of my department's work - being in control of the patches.

You will always be able to break in - there is no 100% solution. You could stop anyone from entering this building, but one of my co-worker's girlfriend showed up and said, "I need to talk to Burton." They let her in. Perfect social engineering.

In our hospital system, sadly, we have not been allowed to use what's called NAC (Network Access Control), which would mean that if you have PC #1 plugged into that outlet, no other PC would be allowed. That's how you should do it. But we have over 6,000 PCs and a few hundred thousand pieces of medical equipment that are being moved around. If we started blocking connections, people could literally die. We would love to implement NAC, but my guess is we're at least ten years away from being able to do so.

We can block specific devices that are attacking us - for example, if someone walks around until they find a free network port, plugs in a Raspberry Pi, and uses it to attack. We can block that specific MAC address. We can block specific ports, but we cannot implement a general whitelist system. We do blacklisting instead of whitelisting. I would love to be able to say "this is the only thing allowed," but we can't. That's one of our problems.

For handling emergencies, we have public procedures available for everyone. Every computer in our hospital system has a shortcut on the desktop for emergency procedures. If we get ransomware and our entire network goes down, we need to know what to do other than check the network drive (which would also be down).

Inside this folder, we have documentation about long-term IT problems, shortcuts to safety information, tips and tricks, documentation, phone books, and emergency order procedures. We have a list of phone contacts, emergency schemes for specific platforms where you can record

data to input when systems are running again, and specific procedures for each department like pathology.

Everyone has access to these resources, even if the entire network is offline. We do weekly tests and yearly comprehensive tests of our procedures. From my department, 3 or 4 people attend these because we have a significant role. Back in the old days, it was just me, but nowadays we're trying to train more people.

We simulate scenarios like: "The internet is down. What do we do?" We talk to representatives from all the emergency areas. Since we use IP phones today, if our network is down, our phone system is down. How does emergency service (112 and 1813) work then? They default to cell phones.

We have press contacts to manage communication during an outage. We have emergency websites where people can look up information. We have pre-prepared press releases saying we're down and working on the problem.

For example, when Maersk was hit by NotPetya and went down for several hours, they quickly published a statement saying what happened and what they were doing. We have similar templates ready. There's nothing worse than saying, "We're down, we don't know what's going on, and we can't figure out how to tell people."

Some years ago, a municipality got hit by a nasty virus. They were down for 30 days. They were responsible for many things, including schools, libraries, and daycare centers. They had two employees taking taxis and cars around to all the schools, daycare centers, town hall, and other locations, putting up printed updates about the daily status. They didn't have phone trees or anything ready. We have those resources and test them rigorously.

We also have comprehensive documentation about what happens in case of fire, who to contact, who shows up, how to communicate, and how responsibilities get transferred. After 12 hours maximum, we need to change the emergency details and potentially transfer responsibility to someone else.

If this building goes down for an unforeseeable time, our service desk will move to another location. We have another place where they can sit and work.

For cybersecurity incidents specifically, we have procedures for every department defining their role and function. We document:

- What happened
- How we found out
- When it happened
- What's affected
- What the damage is
- Whether it affects daily hospital operations
- The source of the attack (internal or external)

- The type of attack
- Who needs to get involved

We work with our suppliers who will help if needed. We check our antivirus, check our logs, check our email, and talk to our technology center about our firewalls. Once we have control, we analyze what happened and how to clean up afterward. All of this is documented and regularly tested.

In most cases, we don't get that far with incidents. These procedures are for major problems that would shut down hospital operations for days.

Interviewer: Is it possible to get this guide?

Expert: You cannot get this one because that would be confidential. You can get the one for the hospitals themselves. Do you have access to the Hope machine? If so, you already have it on the laptop or desktop. It's called Footlocker. Every department has their own procedures documenting what to do if something happens.

I had a good example some years ago when we had to update our Excel with our switch rooms. This would take the entire building offline for some hours, including the emergency room, which is not ideal. Normally we did this on weekends, but that's not a good time for emergency rooms. So we talked to the person and asked when they wanted this done. They said the night between Monday and Tuesday from 2 to 6 AM, so we scheduled it then.

Interviewer: I just want to have it.

Expert: You don't have it? You can get a copy of what I have. We don't put the entire thing in your papers, but you can use it to see what we're doing.

Interviewer: Yeah, because I'm not going to use any product.

Expert: Exactly, you just need the general information about how they're doing it, which is not a problem. I'm surprised you don't have it. I thought everyone had it. It might only be the leaders who have it, but I'll make sure you get a copy.

Interviewer: Because I'm going to send you the information that I know is okay to review.

Expert: That'd be great. I would have asked for that later, but it's not a problem.

We have something called the hard drive where we can share files between people in our network. It gets cleaned every morning. We have a folder called "Feeder Fixing" on our drive that can be seen by everyone. If the file is too large for email, I'll put a copy there. The email size limit is just over 50MB.

Expert: I used this a few years ago when we had to work on the intensive care unit. We talked to their bosses and got agreement. It was put on the internet and sent via emails to the department. We sent an email the week before and the day before as reminders.

We called them two months before saying, "We're going to have one machine we're keeping alive. We just need to take it offline for two minutes to put in a new switch." When we called them on the day to say we were going to do it, they responded, "What are you doing? Cutting into it? You can't do that!"

We reminded them we had agreement for a month and asked about their emergency procedures. They had no clue. Much later, we did work for the heart monitor systems, which involved the same department. We had the exact same problem - they didn't know their emergency procedures.

Every department nowadays needs to have their own procedures. My wife's department found out that they had a lot of physical equipment lying around for emergencies, and half of it was expired. This is something departments need to review: what do we do if we don't have internet access or access to anything for a while?

Expert: We have backups of everything now. For some years, we didn't have backups for our network drives, only the drives where we have patient data. Someone decided the department drives weren't important, but if you asked any department, they would disagree very loudly.

The problem now is with our data storage. It's ridiculous how much data we have - several petabytes. We're facing physical space problems for racks with disks. We just bought new storage again, and it's expensive.

We're also trying to limit people and say, "What should you keep?" We are very open - you're allowed to use computers for personal use, but there are rules that allow us to tell you to delete non-work-related content if needed.

We had one time where we ran out of space on the personal drives. I got the job of figuring out who was taking up space. I found people with 300GB of personal computer backups, 300GB of vacation pictures, or in one case, gigabytes of pornography. That content was deleted really fast.

Expert: Our biggest problem is users because they will click on anything without thinking about it. It's gotten much better. When I started, we weren't allowed to tell users anything. Nowadays there's actually a video about IT security, and we try to do campaigns as often as we can.

We're only allowed one hour per year for training, and you might ask why not more? Because one hour a year times 50,000 people represents a lot of nurses' and doctors' time - that's why we're not allowed more.

My department would love to do a phishing campaign. But with 50,000 people, let's say we target 5,000 people. Our cleaning staff don't even log in to their emails, so maybe half of those

5,000 would check the test email. If half of those who check become worried and call our service desk, that's 1,250 calls during a few days, putting pressure on everything.

We can't just hire temporary workers for this because they need to know our systems. So it's not trivial to do a simple thing like a phishing campaign.

Interviewer: How do you think cyberattacks on hospitals and healthcare systems relate to cyber warfare? Do you consider it a global issue or a local issue?

Expert: Both. It's a global issue in terms of money - attackers who are after money will hit us like anyone else. But nowadays we're also targeted for specific attacks. Russia would be interested in creating problems. We do see attacks from Russia. We had Iranians taking down systems some years ago. We see attacks from nation states.

Russia is a big worry right now due to the Ukrainian-Russian war, but I would say North Korea, China, and Russia are the three biggest threats. North Korea tends to hit Asian countries more, but Russia is a problem.

Interviewer: Are those cyberattacks more political?

Expert: They're very political. Right now, if Russia can change public opinion, that's perfect for them. If they can take down hospitals, power supply, or water supply, then people stop caring about the war because they care about their own welfare: "Do I have heating? Do I have water? Do my hospitals work? Does my power work?"

If those things don't work, people might say, "I don't care about the Ukrainian war. Maybe Russia isn't so bad. Maybe we shouldn't provoke them." That's probably what Putin is going for - to scare countries into not reacting. Like his threats of nuclear war, cyber attacks on hospitals are part of the strategy to scare people.

Expert: Earlier, hospitals were basically off-limits. We would get hit by random attacks because our work email ended up on some list, but hackers wouldn't specifically target hospitals.

That changed a few years ago when hackers attacked a German hospital. They thought it was the university next door with the same name. A woman died during transfer to another hospital, and Interpol handled the case as manslaughter, saying it wasn't just a cyberattack but a criminal case with much more severe punishment.

The police are taking a harder stance, saying if you attack a hospital and risk killing people, it's a much more serious crime than attacking a library. But it won't stop people. Even until two years ago, there was a code that "we don't attack hospitals," but that's gone now.

Earlier this year, there was actually a cyber gang whose leader said, "I'll buy support from you, we'll check through your network, and then you pay us half the money." They even said, "Forget all our customers, we'll steal all the money." The concept of the "honest criminal" is gone now, which is why we've drastically increased our staffing and investments in cybersecurity.

Expert: Between 2015 and 2017, we were hit with ransomware attacks every week. My co-worker and I made a lot of money that year in overtime because we spent at least 50-60 hours a week cleaning up. After we got new antivirus, that stopped.

But I'm not saying it can't happen again. It will happen - it's just a question of time. We have very good security, but things can get through, especially since we have physical access issues in our buildings. It's much harder to attack when you have to use your security card to get in, but we don't have that level of protection. One day someone will exploit that vulnerability.

Interviewer: Is there any strategy to predict attacks or identify the weakest points in the organization? What are these points in your opinion?

Expert: We get DDoS attacks on a regular basis, but we have suppliers who do a fairly good job protecting us. There was one incident recently where we were down for 40 minutes because attackers used a new method that hadn't been seen before, so our automatic defenses didn't trigger. They had to do some manual work, but in general, we're very well protected against DDoS attacks.

We also have very good malware protection nowadays. My biggest concern is physical security. If someone can bypass 80% of our defenses simply by connecting to our network inside the building, that's a serious problem.

We can't solve it completely because we would need to close every door at every hospital and have security guards checking everyone, which would be unacceptable. If you're in line at the emergency room with a broken leg, you can't wait for security to let you in - people could die.

We're working on isolating different hospitals from each other so if one hospital gets hit, the attack won't spread. But it's a work in progress because it affects every program we run, and we have over 4,000 approved programs in our network.

Interviewer: Since you mentioned hospitals, I read that you're managing 15 hospitals. How would telecommunications between hospitals be affected by a cyberattack?

Expert: Very easily. We've switched to IP phones, so if our network goes down, so do our phones. We recently moved to cloud-based call centers, which means we can access them from outside. Before, if the hospitals were hit hard enough, we wouldn't be able to access the call center control systems.

Last month, we had an attack where we were down for an hour in this building due to a massive data stack attack. To stop it, we cut all non-Danish traffic. But that also cut off our cloud solutions for antivirus, our call centers, and services like Office 365 and Teams. We're looking into whether we can keep specific servers open while shutting down other connections, but you don't see the problems until you pull the lever the first time.

Interviewer: Would patients be directly affected by a cyberattack, or would only the organization suffer? What would it mean for regular citizens?

Expert: It depends on how the attack hits. If it's a DDoS attack on our normal websites, it's not critical - you might not be able to see the hospital map or contact info, but that's just a temporary inconvenience.

If someone's platform is down for a day, it's a problem but not life-threatening. If the entire network is overloaded like what happened recently, it causes problems until we resolve it. That particular attack didn't affect patient systems, but it did impact instant communication systems.

If the phone systems go down, that would be a serious problem. We would default to cell phones, but we don't have 51,000 cell phones lying around. Some departments have maybe 50 phones available, but most won't pay for that expense.

On the positive side, many employees have work phones, so a portion of staff would still be able to communicate. And most people carry personal cell phones, which they could use if necessary. Calls in Denmark are free regardless of whether you use your personal phone for work calls.

We also have emergency communication channels and a list of contacts for all our partners. The main emergency numbers would still work, but you might not be able to reach specific departments.

If the entire cellular network in Denmark goes down, that's beyond our control. We do have some radio communications with senior radio systems that connect with ambulances and other emergency services. They test these systems monthly to ensure they work, though the quality isn't great. It's strictly an emergency feature.

Interviewer: What would be your responsibility while there is a cyberattack on CMT? What will be the protocol for emergency response?

Expert: First, we would try to determine what happened. My partner would be the most likely candidate to look into it because we handle operational security. We would start investigating: What happened? Where did this happen?

If it's a data attack like the most recent one, our team and our supplier (which I'm not allowed to name) would examine our data traffic to identify the source. If it's a virus attack, it would be my responsibility as an enterprise manager.

We would then assess what the attack does and what we can do about it. And if necessary, we work overtime. I have time - as you can see from my calendar, I have plenty of availability.

Expert: What we have in “Hospital A” is enhanced resolution, which means we can see everything that happens on a machine. And I do mean everything. Have you read the rules about who is the best in “Hospital A”?

Of course, we don't spy on what you're doing, but we log everything in case we need to investigate something. I don't routinely see what people do on their machines, but if there's a legal or security reason to look into something, we can see exactly what has been done.

We can see what websites you visit, though not necessarily subsites. For example, if you go to a news site, I can see that you visited the site, but I can't see which specific articles you read. But anything related to your machine, we can access.

If users report malware, we investigate those PCs to see what happened. Let me give you an example - as long as you don't share specific details, you can mention this incident. We had an attack last week. It wasn't major, but serious enough that we spent several days handling it. It wasn't an attack aimed at stealing data or compromising our systems.

Sometimes when people browse the internet, there might be banner ads that trigger downloads without you noticing. This happens occasionally. Once we had over 500 people who had a specific file downloaded that they didn't intentionally download. In those cases, we can go in and delete the files.

The recent case involved a specific open-source office program called GPS [name changed]. It's from a Chinese company. To be fair, it's not inherently malicious or illegal software, but it's one we don't approve of because they use cloud solutions. This means if anyone opens a document containing patient data, it might be sent to a Chinese cloud.

First of all, users aren't allowed to install programs without permission - that's a major violation. You need to ask for authorization for programs. We specifically don't allow this particular program.

In this case, we identified where the program was installed - in the User profile, AppData, Local Software folder. It was trying to be persistent, meaning if you deleted it, it would reinstall itself. That's why we flagged it - we don't allow programs to reinstall themselves automatically, as that's potential malware behavior. So we removed it.

For affected machines, we isolated them and had them reinstalled just to be safe. Now we actually have a check in place that alerts us if we detect execution where the signature from the executable file is from similar software. This allows us to handle these situations proactively.

Expert: This is important because it shows what we can actually do in terms of protection, and this applies to all machines. If I'm worried about my machine, I can select "isolate endpoint." Why do we do that? When I trigger this option, the machine is instantly cut off from being online.

We can still access it through our security tools to examine all files, processes, and everything running on it, but it cannot spread malware to other systems. In the old days, if your machine was infected, you would call us with concerns. We would tell you to turn off the machine and physically disconnect the network cable. We'd put a post-it note on the computer saying "Don't use it," and eventually send an on-site technician.

The problem was that about ten minutes later, someone would often turn the machine back on because they didn't see the post-it note. We had malware-infected machines that were

reconnected to the network because people missed the warning. Nowadays, we can remotely isolate the machine, and even our service desk staff can do this.

So if there's an incident at 2:00 AM where a user is getting weird pop-ups suggesting they might have a virus, the service desk can isolate the machine immediately, and we'll investigate it the next morning. That's how we handle PC security incidents.

Expert: For forensics, when we need to determine what actually happened, it's important to go beyond simply stopping the threat. We need to understand how it occurred to prevent similar incidents.

I'm not a programmer by trade - one of my coworkers is really good at this. I programmed 20 years ago, but I'm not a programmer now. Essentially, our tools allow us to examine processes, files, network event logs, and connections. We can see very specifically what actions were taken on a machine and what happened.

Let me give you an example. We had a coworker who contacted us because while she was at a movie theater, something was posted from her Facebook account that she didn't send. The only computer she had was her work machine, which was in her apartment with her two-year-old and four-year-old children and her ex-boyfriend. It's not hard to figure out what probably happened, but she wanted proof.

My coworker looked at the firewall logs and could see exactly when the machine was turned on and then when someone connected to Facebook. In this tool, we can see that the machine was turned on at a specific time, Facebook was accessed at a specific time, and which programs were started. In this case, no files were saved, which suggests the person might have just browsed Facebook.

If they had also downloaded files or sent emails in her name or saved files, we would have seen that too. We could say, "These items were opened in Explorer, then Facebook was opened, and that's all that happened." So we could determine there was limited potential damage. She needed to talk to the ex-boyfriend, but no significant harm was done to her work account.

We need this capability to see exactly what happened at a given time. I did a small training session on this recently.

Interviewer: Do you do these training sessions regularly?

Expert: The ones I just showed you happen every couple of months, whenever people need it. We've had a lot of interest, so it's done on a regular basis. Some of our infrastructure departments, where we have people who've been working for 20 years and might not prioritize security, also wanted training. So I demonstrated our capabilities to them.

They were surprised, especially about this particular tool. They asked, "You can see that much?" and I confirmed that yes, I can see exactly what's happening on a machine. However, we don't want to be in a position where nurses feel surveilled 24/7 - we absolutely do not do that. But in

case of a security problem or when there's a serious issue we need to solve, or if there's suspicion of a legal breach - like someone stealing files from our platform - we can investigate which specific files were accessed.

Do you remember that case? How long have you been in Denmark?

Interviewer: For two years.

Expert: You remember the case about the 13-year-old girl who almost got raped? We found some people due to that one because some people had been looking into the journal when they weren't allowed to. We were one of the parties involved, and we checked the logs in the emergency response platform for ambulances. Some people got either freed of suspicion or fired because of that investigation.

Some people thought, "This problem is logged in the emergency response platform for ambulances. I'll log in there and check instead." That's going way too far. We spent three days investigating, and we could see everything in the browser logs. That got a few people fired because they made massive privacy violations.

Expert: This next case might be interesting. We almost went into emergency mode. This isn't proprietary information; it's just an example we use to show what we can see. We were this close to taking drastic measures.

Have you heard of something called a "rubber ducky"? It's a small hack tool that can basically do anything. It looks like a small USB device, and if I plug it into a machine, I can do anything—keylogging, hacking, whatever. With some add-ons, you can use it for things like stealing card information if you get near someone for just two seconds. It's fairly dangerous stuff.

We got an alert about a potential security issue. Our data only stays in the systems for three months, so I can't find the specific details now. But we use a framework called the MITRE ATT&CK framework to categorize threats—from reconnaissance to exploitation to malware execution.

This particular incident triggered alerts for reconnaissance (usually port scanning or checking for IP addresses), exclusion (running something during installation), hiding activity, trying to use admin access, and collecting and gathering data—all of this happening simultaneously on a computer in “Hospital A”. With a rubber ducky, you can do payloads, password exploitation, keylogging, whatever you like basically. We had four people investigating this.

Expert: Our problem, as usual, was contacting the affected user. We found out which laptop was affected, so we didn't immediately send someone out. At first, we were afraid someone was trying to steal data.

After five calls, I was lucky enough to know the head nurse in that department, so I called her. She told me the employee was at another department but would be moving to them soon. Four

people later, I got in touch with a close co-worker who told me the employee wouldn't be in for another hour.

So we determined the laptop wasn't in the hospital. Perfect—then it must be either at home with the employee or with her husband. This isn't something that happens randomly. We were talking about possibly involving the police or issuing a written warning if necessary.

Expert: When we found out it was a private matter at home with her husband (who's an engineer), things became clearer. It turns out they have four docking stations and four monitors connected by USB wires in their home office. Her husband was trying to make a homemade keyboard which used the same chipset and programming as the rubber ducky. The USB connector triggered our warnings.

We didn't find any suspicious files on the machine, but the device's attempt to register itself as a keyboard and other peripherals triggered our security alerts. Our systems collect data from multiple sources—we talk to our firewalls and collect data from everywhere.

Expert: We face some challenges with monitoring network traffic. Currently, about 60% of all communications worldwide use SSL encryption, and that percentage is likely higher now. This means we can't always see what's actually being sent. If malware wants to connect somewhere or someone is trying to steal our data, they'll use encryption to hide it.

We're trying to implement decryption capabilities so we can monitor these data streams. However, I wouldn't be allowed to look into the data stream directly. Our software would scan for sensitive information—like if we see 8 or 10 instances of a CPR number (Danish personal ID) being sent to a non-secure address, that would trigger a warning. Even though we have high security clearances (the second highest), we would not actually be allowed to see the data itself.

We've been trying to get permission to do this monitoring for ten years. The main concern is privacy—people are allowed to use their work devices for private purposes, so questions arise like "Can you see what I'm doing with my bank? Can you see what I'm doing on social media?" We need to create filters that exclude financial institutions, healthcare institutions, and similar sensitive sites.

Expert: We're also implementing a system called Cloud Manager to see what people are trying to send to OneDrive and SharePoint. We have Wildfire, which uses the same database as our antivirus, to check all files saved in cloud storage for potential issues. Right now we have 390 flagged items.

The problem is that this requires manual sorting because the antivirus filters flag issues that I don't necessarily agree with. For example, a PC backup setup will be flagged because users aren't allowed to run programs, but that's an easy decision to remove. For other items, like PDF files being flagged, I need to investigate why.

We had a case where students at the school were using a Danish link shortener called ShortLink in their PDF documents. That service gets flagged as a potential risk by many systems. When 15

people started emailing these documents back and forth, our spam filters gave us 15 warnings every time someone replied. I had to write to them asking them to stop sending that file.

Expert: We also monitor if sensitive data is being sent outside our network. I can use this example because there's no patient information in it. We can see what triggers the alerts but can't see the actual email content. We can download the file if necessary.

In this case, we have a teacher who needs payment, so they need to provide their CPR number. That's allowed. The system flagged it because it was sent to an untrusted recipient. In Denmark, we have what's called "e-Boks"—about 3,000 domains in Denmark are on a network where communication is automatically encrypted. If you email someone not on this list, it's potentially readable.

If a doctor downloads a patient's journal and sends it to their own email, that's completely within their rights. But if they send a patient's journal to their personal Gmail account, that's a privacy violation. That's what we look for.

We only check for CPR numbers because there are many false positives with other identifiers. We also run into issues with profanity filters since words like "slut" will trigger warnings. We don't care about minor warnings—we're looking for actual data breaches.

Expert: If we find a doctor sending patient data to an unauthorized email, we'll call them and say, "By the way, this is a violation. We don't need to escalate this if it's a one-time thing, but please don't do it again."

I had a case where a doctor had a secretary in another department package 12 journal files spanning a nine-month period and send them to a personal email. That's not a single-time use—that shows a systematic breach of protocol. That case went to the lawyers because it was serious enough to warrant formal action.

Nobody is interested in seeing everyone's emails—we only care about the triggered warnings. I had one case where a professor fell for a phishing email from Norway, sent it to her husband who's a lawyer, and he also fell for it. I had to call both these highly educated people and tell them they'd made a mistake.

Education level doesn't matter when it comes to security awareness. There's absolutely no difference between doctors and cleaning staff in terms of likelihood to fall for scams. We're generally very nice about it—we don't fire people unless the violation is extreme.

I had a case some years ago where staff were sharing logins because they were bored during night shifts. They put pirated movies on someone's personal drive and had a list of DVDs they were selling copies of. We identified four people involved, and they received written warnings. You need to do something quite serious to be fired immediately.

Interviewer: Who are the main victims of cyber attacks? Who suffers most from them? For example, if a nurse gets a phishing email and clicks it, what data would be compromised? Is there any connection between work computers and personal phones?

Expert: We actually try to separate those systems quite well. I have a work phone that we're allowed to use privately. If it's installed on my private phone, it creates two profiles—personal and work. If I take a picture on my phone and want to share it via Teams, I actually have to specifically grant access to my personal area to get the file.

Phone-wise, we have a fairly separate system. I'm not saying it can't be broken, but I'm not particularly worried because there's fairly good software in place. In Asia I would worry more because people tend to jailbreak their phones and not pay for apps, thus getting infected. We protect our phones from jailbreaking, which stops most problems.

To infect a phone, you basically need to encounter something that Google or Apple missed in their app stores. If I get a suspicious PDF file, I might open it on my mobile phone because that can't really compromise much. But an infected computer is much more concerning, especially if it enables keylogging or credential theft, because then attackers can access your email and network drives.

If I walk into a department pretending to be from IT, I could likely gain physical access to a machine. If I have someone's login credentials, I can access all their documents and start stealing data. That's especially problematic when people don't lock their computers when stepping away. My wife's department has this issue—she tells them that if patients access the unlocked machine, any actions will be under the employee's name.

I'm not too worried about nurses specifically. What we've seen so far has mainly been ransomware attacks or phishing emails. You're not allowed to have patient information in emails anyway.

What would be more concerning is if someone infiltrated the finance department that handles contracts. They could send an email pretending to be from a vendor like Siemens, providing legitimate contract numbers but requesting changes to bank details for payments. That wouldn't be noticed until Siemens asked why they weren't receiving payments.

For patient information, you would need physical access to a machine and also need to break additional security rules. We use two-factor authentication to access critical systems, so you would need both the login credentials and the phone receiving the verification code.

I'm actually more worried about physical threats like the "USB Killer" device. If I wanted to cause damage rather than steal data, I could use a device that costs around $100 that sends a power surge through USB ports to fry motherboards. If I did that to 20 machines and moved on to the next hospital, I could cause millions in damage. Who could stop me? We don't have comprehensive video surveillance, and we don't block or secure all USB ports.

The only protection would be extreme measures like gluing keyboards and mice to laptops, sealing all other USB ports with epoxy, and replacing laptops when they fail. I'm concerned about this because there's no practical way to protect against it.

For patients, I'm more worried about individual personal data breaches. We haven't seen many examples of patient data theft—mostly ransomware. But it's just a matter of time until something serious happens. There's no silver bullet; eventually, someone will find a way to steal something.

I'm also concerned about the consequences for individual users who click on malicious links. Beyond the security breach, we've seen cases where access to email accounts was used for harassment, like sending fake pornographic images to coworkers. I worry about these ethical issues too—it's our responsibility to help protect our users from these situations.

Interviewer: How about the mental aspect of the problem? How dangerous is a cyber attack on the mental health of the employees? For example, would a doctor be worried about getting hacked so that patients cannot get treatment in time for operations?

Expert: I would say the general doctor is not worried about cyber attacks. We have our emergency plans and designated people who worry about how to handle these situations—that's why we test and practice response protocols. The typical doctor wouldn't be that concerned.

They might become worried if they see news about attacks, or if we increase our cyber security evaluation level to "very high." This can cause some mental stress.

We have had situations where people get paranoid. I had one case where an employee had reset two phones and was worried about hacking on an old Nokia non-smartphone. He thought it was being hacked because it started blinking whenever he went near the airport. Sometimes worry can lead to paranoia in employees. While that's technically not my department's problem, since it involves IT situations, we try our best to help people and reassure them there's no need to worry.

Interviewer: How would you ensure their safety, and would you provide some training materials?

Expert: We would normally not be allowed to train outside our department. This type of information is internal, which is why you needed to ask specific permission. Normally we wouldn't share these details externally, but in situations like CEO fraud, I've spent time explaining to people what happens.

I made a small presentation about CEO fraud for central staff members to show them what it looks like and how it works. Whenever people are targeted by CEO fraud or we see attempted attacks in our spam filters, we know they've become a target and will likely be attacked again.

I'll talk to them and ask if they want me to cover this topic in their department meeting. I'll say, "We've seen attacks targeting us. You need to make sure you don't transfer money without speaking to me directly," and use real examples of what happened. This helps people understand the risks.

We don't do hardcore training programs. For people who seem paranoid, I'll explain what happened, how they can protect themselves, and basic security practices. But we don't provide intensive training for individuals.

I would be very happy if someday we actually had proper training when people start. Currently, we basically say, "By the way, you have OneDrive and you have P drive. Good luck." That's what happened when I started, and it hasn't improved in over 20 years.

The problem is that training falls under individual departments' responsibilities, so we can't force them. We can provide one-hour annual training videos, and we're trying to work with other departments. We've created some training videos to explain concepts like phishing—how it works and what to do about it. We've made two or three short videos, about 2-3 minutes each.

Interviewer: Is this public or private information?

Expert: It's internal to the hospital. You wouldn't be able to access it directly, but you can mention that we have these videos. There's nothing proprietary in them. You could probably use them if you wanted to—there's nothing sensitive in them.

[*The transcript includes Danish language content describing a phishing training video. The video appears to discuss phishing attacks, CEO fraud, statistics about phishing emails, and best practices for protection.*]

Expert: You can use that information if you want—there's nothing confidential in it. We've made two or three of these videos so far.

It probably started as an inter-departmental issue because security training technically belongs to the Information Security department. When we started making videos, there was some tension, but I think it's worked out by now. We've created a few videos, but we're not allowed to send them to everyone. We can put them on our website for people to view.

We have one hour dedicated to Information Security's responsibilities. We try to educate people when we see them doing something that breaks the rules. For example, with the case I mentioned where someone downloaded Chinese office software, they received an email saying, "You're not allowed to use non-approved software."

We also see people trying to install VPN software. We've blocked this on all laptops because it would conflict with our systems, but we still had 49 attempts last month. We're trying to automate responses so when we detect downloads of files with certain names, the user automatically gets an email explaining they're not allowed to use unapproved software, with a link to our rules. We're trying to educate people through automation so we don't need to talk to everyone individually. But education is not our main focus—that would be Information Security's responsibility.

Interviewer: But back to the rubber ducky—as far as I understood, the Rubber Ducky is based on Raspberry Pi software. Which software tools are most popular for producing attacks?

Expert: Honestly, I have no clue about the specific software. Attackers usually work with their own custom software. The most problematic attacks are the ones trying to appear legitimate.

For example, the Chinese software we just discussed isn't approved, and if anyone opens those documents, they might lose data. There was an attack recently that failed by pure luck. Someone, most likely Chinese, targeted a specific sub-program for Linux that was maintained by just one developer on GitHub.

The attackers created 3-4 accounts that all contributed useful software on GitHub to build their credibility. They spent over three years infiltrating this developer's trust, with their accounts saying things like, "Why don't you update more often?" and "I have some free time, I can help." They managed to push enough to get one of their accounts added as a core admin, and then added a small keylogger into this widely-used program.

It was only discovered because during beta testing, someone at a company (I think Microsoft) noticed a 0.02-second delay when performing an action. They investigated deeply and found the keylogger in what appeared to be legitimate, trusted code.

That's where the real problem lies—when someone can insert malicious code into trusted software, like the backdoor that Microsoft/NSA had which led to the WannaCry and NotPetya attacks. Vulnerabilities in proprietary or open-source code that people trust are the biggest problem.

We're becoming skeptical of GitHub. It's great, but who controls it? Can they change what you do there? We had a case with a developer who used the Escape key a lot but found it awkward for touch typing, so he used a GitHub program to remap his Escape key to Control. The problem is, GitHub was logging which keys he was pressing—that's essentially a keylogger. It would take about two lines of code to turn that into a malicious keylogger. How much do you trust that system? We don't.

He had to uninstall it. He was upset, but he had installed a potential keylogger with root access. Hackers will develop tools fairly quickly, but if they can hide them in something trustworthy, that's a big problem for us. Another issue is when outdated medical systems can't be updated, so we can't patch known vulnerabilities.

Expert: I hope I've made you a little paranoid—that's usually the case after I'm done talking.

Interviewer: Actually, this information was very helpful.

Expert: I was wondering how you could use it, but anyone can learn from this.

[*The interview ends here*]