#116 - A European view of CISO responsibilities with Michael Krausz

[00:00:00] **G Mark Hardy:** Hello and welcome to another episode of CSO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today and am pleased to have with my on this virtual studio here, Mr. Michael Krausz.

He's the Chief Executive and Chief Consulting Officer of the ISC group. Unless you think he's in the next room over, he's actually over in Austria. And Michael and I worked together a number of years ago and I was incredibly impressed with his skill and his knowledge of a lot of things cyber. And it's just a real privilege to have you on the show today.

Welcome, Michael.

[00:00:47] **Michael Krausz:** Thank you, G Mark. It's a privilege for me to be here. Thanks a lot.

[00:00:51] **G Mark Hardy:** Now, we were talking before the show about the fact that you've been around a long time. Can you tell folks a little bit about your background and what brought

[00:00:57] **Michael Krausz:** Yes, of course. No, I'm happy to. I'm just giving [00:01:00] you the full story here. It basically started when I was six because back at six I wanted to become a detective, like a police detective. At 13, I wanted to become a lawyer, and at 14 I got my first computer. And the first program I wrote was actually a program that analyzed Latin works.

So for instance, you would enter La Detour and the program would say this is the third, conjunction of present tense in the subjective passive voice. From then on I was hooked, and I was hooked to security from a really, very, very early age. And when I graduated from high school, all these studies programs that exist today simply didn't exist.

So I was like, what the hell do I do now? I know I want to do something with security, public service, like actually becoming a police officer. Doesn't pay well at all. So now I'm not going to do this. So basically I started physics, computer science, and law in order to, satisfy my passions.

That's, that, that's it, really. [00:02:00] Right? And then I, I still remember like at the age of 22, 23, going to university and asking myself. Who in the whole wild world will ever pay me for the service I intend to provide to the world, which was some kind of security consulting, and then in, in 96 I was sitting in front of my computer at the university's IT center at which I was working, and Checkpoint came out with the first firewalls. And I had this gut feeling that said yes, security will be big one day and 25 years later, like in 98, I founded ISC Group. And 25 years later yes, it is really, really big. It is the one topic, you can't ignore anymore. I mean, it was a hard uphill battle to get to that point. When I, when I do company presentations today, and the first, the second slide shows, we did projects in 32 countries on four continents. But why, why the heck did we do that?

Because in 98 in Austria, nobody cared [00:03:00] about cybersecurity. Simply nobody. So we basically started our company in practical terms, in Germany, in Switzerland, in the UK, in the US yeah, but not in Austria. And it took 15 years for the market in Austria to be mature enough to actually sustain the company.

Right. And that's the whole story. Since, my favorite fields of studies from these three was actually law. So it was really a small step to, to venture into the standardization world because the standardization world is all about language.

It's all about meaning, about context, about grammar and syntax, same as law, really. Right? And of course, I do have a very strong technical background because I, I worked at the university in IT center. I was a system admin, I was an IT manager. I was a security manager in my employed positions.

And then in 98, I made the cut to become self-employed, started a company. And yeah, here we are, 25 years later. And frankly speaking, information security provides a very, [00:04:00] very, very nice and income now

[00:04:01] **G Mark Hardy:** That's true, true for a lot of us. And yeah, I was also, in this area, even earlier than that, and I kind of liken it to the California Explorers who went out in the 1820s looking for gold. Now, they didn't starved to death or get eaten by bears by 1849 when the gold Rush comes out.

They're the old guys going off my lawn,

[00:04:19] **Michael Krausz:** exactly. Yeah. Yep.

[00:04:20] **G Mark Hardy:** But you, you'd mentioned about standards, and we're gonna talk about a number of things, but I think we gotta go to that first because you said it was similar to law because a lot about language and meaning, and where we first met several years ago was working on a project for an American company that.

Was trying to close a deal over in, I think it was Germany. And what happened was, is just toward the end of the contract, it was like a big sale that the German company said, yeah, just send us a copy of your ISO 27001 certification. And they like, yeah, no problem. So they call up their auditors and they said, Hey, we have a requirement for this ISO 27001 certification.

Can we have one by Friday? They're like doesn't work that way. [00:05:00] Said,

what

[00:05:00] **Michael Krausz:** Yeah, no.

[00:05:01] **G Mark Hardy:** a lot more involved. He says, well, you need to get somebody. So I got the call, I got referred over there, and then I like, okay, fine. Call this G Mark Guy. He knows what he is talking about.

Well, I know a lot, but I also know what I don't know, and I'm willing to admit that. And so via a mutual friend that got ahold of Michael and I said, Michael, can you help out here? And so what he had structured was a gap analysis. I'm telling your story, but I'm telling it from my perspective where he had gone through and set up of the number of criteria, looking at the ISO 27001 requirements, looking at the practices they were doing and if they were doing what it required that was green and if they weren't doing it, but they should be doing it. I think that was yellow. And what I remember, which was innovative was if they were doing the opposite, that was red,

[00:05:45] **Michael Krausz:** Yeah. Yeah. Maybe a little bit of detail here. So, when we do a gap analysis, we basically have four levels of fulfillment. Green, yellow, orange, and red, and basically three dimensions. Policy, practice, proof, I mean, you should call it evidence, actually, but not [00:06:00] proof, but you know, we call it proof because it sounds better.

Policy practice proof, policy, practice proof. That's the iso engine policy, practice proof. And the proof, the evidence of what use are doing either exists or doesn't exist. That's easy. Now the practice needs to be either risk adequate or it isn't risk adequate. Right. But for a policy, the evaluation scheme in itself is a lot more complex because what you mentioned happens exactly there, if your policy exists.

Okay? Your green? If, your policy has minor gaps, no worries. You're yellow. If your policy is missing, that's a red. Right, but the worst case, it's actually not a policy missing. The worst case is a policy existing and not being adhered to. And there can be minor non-adherence or there can be major non-adherence.

Jokingly, I always say if there's a major non-adherence, either your policy is stupid or your people are stupid. But in fact, of course, we need, you need to know the root cause of that because you know your policy might be bad, your [00:07:00] people might not be properly trained, your people might not have their resources to execute the policy, and so therefore, this kind of worst case when it comes to policy adherence is something you should know about and you need to tackle that.

And tackling that is a lot more complicated than just writing a policy that isn't there because if you're in a greenfield situation, you can basically do what you want as long as it makes. So overall, if you think of these three dimensions, policy, practice, and proof for iso in the ISO world, it's actually most important that your practice is risk adequate.

So if you, if you have good practice, no policy, and you, but you can demonstrate the practice, you will never be red in a gap analysis. You will be yellow or orange, right? However, if all three elements are missing, then you're. Right, because you need to at least have to practice and at least show that your practice that you put some intellectual work into why you are doing exactly.

Where you're doing stuff exactly that way. So this [00:08:00] is how this kind of classification scheme or evaluation scheme of gaps actually works.

[00:08:05] **G Mark Hardy:** And, and that makes very good sense. And it's interesting because what I found interesting is this American company seemed totally befuddled about a requirement for ISO. We're like, oh, SOC 2, SOC 2, it's the American way to go, but yet Europe like SOC, what?

[00:08:20] **Michael Krausz:** Exactly, exactly. It's, the situation is basically the following. Frankly speaking from our point of view, the US is an island very far away and from the US perspective, Europe is an island very far away. So the point is this, like in Europe nobody knows about SOC 2.

Some bigger companies do. But nobody requires from another company to have SOC two because the whole ISO World International Standardization Organization, which was founded in Geneva, it is basically ISO is a European invention. And of course, therefore, ISO standards will always take precedents about any other standards.

Well, in the US of course, nobody really knows the ISO standards unless. You do business [00:09:00] outside of the US for instance, in Japan because the Japanese love the ISO standards or in Australia or in Europe, right? And this is where the requirement comes, or this is where, this is why this is so different. And the basic, the basic difference in thinking is that ISO standards tend to prescribe the achievement of certain goals.

Or objectives, but they don't tell you how to do it. You're completely free to do it in any way you want, as long as that way is reasonable, and in my auditor role, I always say, as long as you're not doing something obviously stupid, it's okay. Right? Because we assume that you're putting an honest effort into actually achieving the goals.

Well, if your effort is not honest, the auditor will know while, for instance, while on the other hand in the US people are not comfortable with that. NIST CSF, for instance, is extremely well thought out, but it's also extremely heavy. If you print it, you can actually kill somebody with that.

With iso you cannot kill anybody because it's just 30 pages, 35 [00:10:00] pages. So NIST CSF has the advantage that it's really, really prescriptive. So , if basically your mindset revolves around, I need to know what I need to do and not what I need to achieve. Then NIST CSF is a really good choice, but it just takes two to three years to implement it correctly.

Right. So this is, well as maybe even a difference in mentality that comes from the fact that American companies are really, really careful and conscious about not being sued. Because the US itself is a rather litigous country. And this is I think where kind of the differences in acceptance come from.

On the other hand, there's also the aspect that SOC two is completely monopolized. The big four accounting firms basically hold even a copyright on SOC two, so to speak, or at least on the under underlying standards. And therefore it's, for them, it's just a business model. Right and I don't really like that, I like standard standards to be public, to be publicly understandable, and not to be monopolized by an oligarchy

[00:10:58] **G Mark Hardy:** Now if we take ISO [00:11:00] 27001 and we look at this ancestry, it was ISO 17799, and before that it was British standards, 77 99. And if we kept going all the way back in time, till one of the first real security standards that came out. I think you have to go back to around 1983 to 85

[00:11:18] **Michael Krausz:** oh, oh, I wouldn't actually, I wouldn't know because at 85 I was just, in 85 I was just, doing my Latin analysis program. Right. ,

[00:11:25] **G Mark Hardy:** I remember getting my first copy of the Orange Book.

[00:11:28] **Michael Krausz:** Oh yeah, yeah. But see, oh yeah, just, just a little thing here. so ISO 27001 goes back to BS 77 99, which was a British standard.

And one of the funnier aspects here was that when it became an ISO standard in the year 2000, they basically just copy and pasted it, because the British wanted it to be in ISO standard, and it was a good idea to do that. Now, back then, The ISO standard had a rule in regard to HR security, that you should collect character references from anybody you intend to employ, which for the British is [00:12:00] a very, very, very normal thing for any other people in Europe.

It's not, it's absolutely offensive. To ask for character references, . So, after a little bit of discussion, and it didn't take long in the 2005 five version, that requirement was dropped. It no longer exists. I just told you to illustrate that even, of course within Europe there are mentality differences that then find a way or let's basically cause discussions on or when it's about standardization. Now getting back to the Orange book, I remember when I started, so I started my studies in 90, in 1990 and I think in 1992 I came a across the orange book and I was really, really impressed. Cause I mean, it's not really a security standard because it doesn't have the breadth of ISO 27001, but it's more like a classification standard.

Right. And for instance, even today, you could, when it comes to chapter eight, asset classification handling, you could use the orange book as a classification [00:13:00] guideline. It's really good, and I was really impressed by the structure, by how beautiful it was from a systematic point of view and kind of how close to practice it was.

[00:13:12] **G Mark Hardy:** And it's interesting because the orange book was written before we really network anything.

And so as a result, I remember there was a saying we had back in the eighties, the federal government C2 by 92. Yeah. How are we doing on that? And of course, what happens? We came along in the wave of networking and then we started going through the whole Rainbow series of books.

And I'm thinking of doing a an art, an episode on Raiders of the Lost FIPs. I'm gonna look at all the old federal information processing standards. I got my Rainbow Library. That I have to dust off. I think there's a red book that came out. It was the first draft version. I only paid in a hundred copies of that.

That was the first network standard. I have one because I was working with the groups back then around 86, I think it was 87. We started thinking about what do we do when we connect these things? And of course, The problem has expanded tremendously, and now we're at the point now where [00:14:00] businesses have to have IT to be able to pretty much get anything done unless you're doing a SOD business and even then you're probably gonna have QuickBooks or something as an accounting package.

But as we look at them, the parallel development between the US with their NIST standards and their SOC 2 and things such as that, The rest of the world, as we like to say, if you owe the ISO standards and things like that, do you see that as being permanently divergent? Do you ever see it almost like a reunification like Germany West Germany was able to do.

[00:14:31] **Michael Krausz:** The funny thing is that, for instance, if I look at the ISO world, in the ISO world, it is very common to have accreditation bodies. And the accreditation body basically sets the rules for the certifying bodies on how they actually certify the customers. Now, fun fact, until about three years ago, the US didn't have an accreditation body.

Everybody could do whatever they wanted, but now they have one. And I personally know the people who act, for instance, do the certifications for Microsoft and for Google. [00:15:00] And so from this point of view, you are kind of right that on that level, they're kind of growing together interestingly by the US adopting European practices.

On the other hand, I think, it's really a matter of angle of view, so to speak, because in the ISO world, we try to be rather abstract. We focus on the goal and the objective, and we let you define the way. Whereas, as I said, the US mentality is also more like, let's define the way in advance.

Let's plan that, let's optimize that and let's be clear about what our way will be. So this is a fundamental difference that from my point of view, can never be bridged. And it won't because it's like a cultural difference. It's not an intellectual difference, so to speak. Right? And and one thing that happens, of course is, or that could happen. Depending on basically the level of abstraction you, you work on on that, on each level things can come together, but more or less [00:16:00] not in the big picture. I mean, the needs are basically the same. We have a need to secure our networks. We have a need to secure our applications, our people. More or less our physical environment.

But how to do that is, is really a matter of hard debate. In the ISO world, the one principle so to speak, is that you should act according to your risk profile, establish the risk profile, and basically that puts the owners to know what that is on you. Whereas, for instance, even the German Baseline protection manual or this C S F, they rather take that a little bit out of your hand by being very prescriptive about what you need to do.

And of course there are areas where you should be, like for instance, when we think of the OWASP top 10, top 20, I mean, there's no need for convergence. The convergence is there. We all follow the same rules in that part, but where we don't follow the same rules, that's when it comes to the organizational part of things.

[00:16:57] **G Mark Hardy:** Yeah, it's interesting. There's an old apocryphal [00:17:00] quote, it was actually attributed to a, a German officer in World War 2. He said one of the serious problems in playing to fight against the American doctrine is that the Americans don't read their manuals, nor do they feel any obligation to follow their doctrine.

And this almost seems now, 80 years later, that we sort of traded places.

[00:17:16] **Michael Krausz:** On Monday I met with a former SA soldier from the SAS, and of course we were discussing Ukraine a little bit. And the very interesting thing he said is that Ukraine, 15 years ago started to train the soldiers according to the old British model, which is to give every soldier the intellectual capability to be at least a troop leader. Meaning to enable them to make battlefield decisions when they need to be made. Whereas the Russian Army, it's just a big, monolithic, hierarchical pile that, doesn't amount to anything these days, as we can see.

Right. And of course, enabling people to make their own decision at the time when they need to make those decision is simply the superior approach. And so

[00:18:00] therefore, if you don't read the manual, but act on impulse or act on what the battlefield at that point in time requires from you, that's actually the superior approach as we have seen

[00:18:09] **G Mark Hardy:** And, and, and we saw that in Gulf one where they had embedded units like from CNN and the like. And then we, we kind of nicknamed it, it was the Sergeant's War or the Corporal's War. And the reason being is these non-commission officers were making battlefield decisions. And there's somebody there with a camera rolling.

And the word might come in from the hierarchy is that there's a sniper in the tallest building. In the village, go blow up the building. And then you go there and you find out that that's where the village elder lives and his mother lives there and the family's there and sniper is long gone. And you say, I'm not gonna blow up the building because first of all, it doesn't do anything militarily for you.

And secondly, you just alienated the entire population of that town against you. And so by being able to empower that, but of course there's a risk. In doing so at the higher levels in that you look at what happens from the [00:19:00] perspective of will your people make the right decision,

[00:19:03] **Michael Krausz:** You are kind of putting, putting your finger in the wound here because, one of the big open problems in cybersecurity is situational awareness. The US to did a really, really good job. If I think of those fusion centers that were established after 9-11, where basically all the security services come together to discuss the situation and, and build situational awareness, which for every company today is still a challenge. How do you know what's going on in your network?

Right?

And, we've come a long way with SIEM technology and SOCs and stuff. We are not where we should be. Like I always compare. I like to compare it security to radio activity. If you don't measure what's going on, you don't know whether you have been exposed to radiation and in IT security, it's the same.

You need to actively look into your network using a SIEM, using a SOC, using all kinds of detection technology to actually find out what's going on. I mean, here's a, here's a little anecdote, right? So I [00:20:00] was actually designing one of, I was one of the designers of one of the very first intrusion detection systems that have existed in 2002.

and we've deployed this with a very big bank. And, you know, back then these IDSs they couldn't do much really. Right. And there was still a lot of philosophical debate o over whether an IDS actually made any sense. So we are deploying it at this bank and we are doing we are analyzing network traffic.

And we find out that a huge amount of network traffic can be attributed to Microsoft Messenger. So, what the hell are all the people in this really huge bank of national importance doing with Microsoft Messenger? Messenger? So then on investigation we found out, well, the bank doesn't have enough meeting rooms.

So whenever people are supposed to meet and because they had no other technology available, well they met on Microsoft Messenger. An external tool run by a third party in whose chat rooms, so to speak, [00:21:00] they had serious discussions about the bank's business , which of course, from a security perspective is a big no no.

Right? But, nobody was aware of that. I mean, of course, know, they all know, knew they did it, but security, the security function wasn't aware of it. The CIO wasn't aware of it. The board wasn't aware of it

[00:21:16] **G Mark Hardy:** Yeah, it's interesting the things you discover. I remember I was working, I had a client one time and I was there on site. I was basically there doing some forensic analysis, so I, I fired a wireshark and I'm going through it and I'm looking, I was like, what in the world is this? I'm seeing IPX. I said, what do you mean IPX? This is like, what? I've got a time portal back to the 1990s and

so. I went looking around and here's what I found it, it was legit and it was also I was seeing Banyan VINES and everything else like that. There was a multifunction printer in the basement that whatever group was the lowest on the political scale in the company.

They got the oldest printer. It still worked [00:22:00] okay. It might have been diesel powered, I don't know. But the thing was, is that it, it was built so long ago. It had all these protocols and it was still on all the default settings, which means no security, and it was connected to the outside world, and it had been there for 20 years, maybe 15 years, and it.

[00:22:19] **Michael Krausz:** So this reminds me two, two more anecdotes here. I'll do the quicker one first. In 2021 we did a rather huge pen test for a critical infrastructure company, the which had an IOT network and the office network.

And we found out that the one thing that connects the office network to the IOT network which was otherwise completely separated, was a printer And if you penetrated the printer, you could. At least, denial of service, the IOT network, which in that case would've had dramatic consequences.

Now, because you mentioned it, I mean, actually you win that race. You win the race For who, who encountered the oldest operating system in the, in the past few [00:23:00] years? Because, like in 2022, what will you, what would you, what's your guess? What's the oldest operating system we encountered in a, in, in a gap analysis?

[00:23:08] **G Mark Hardy:** Oh, let's see. It's probably not as all the way back to cpm, so I'll say Windows 2000.

[00:23:13] **Michael Krausz:** Well, windows NT four.

[00:23:15] **G Mark Hardy:** Okay. 4.0. Yeah.

[00:23:17] **Michael Krausz:** Right. So this year? Just this year. January this year. So three weeks ago, what do you think was the oldest operating system we encountered?

[00:23:25] **G Mark Hardy:** So you'd probably be older than that then I would guess. Yeah.

[00:23:29] **Michael Krausz:** no, but

[00:23:29] **G Mark Hardy:** Next, you know, so Windows Millennium Edition, perhaps.

[00:23:32] **Michael Krausz:** Windows xp.

[00:23:34] **G Mark Hardy:** I still have XP on my left. Look, see this is my artwork. I say art is anything you can get away with.

[00:23:39] **Michael Krausz:** Yeah, and, and see, but see, the very practical problem, the very practical problem here is, is actually legacy systems that you can't get rid of because they're tied to some kind of machinery or equipment, which cost you hundreds of thousands of millions of dollars or euros or whatever. Like for instance, in that case, the XP machine was connected to some laboratory [00:24:00] equipment, which, cost north of a hundred thousand dollars and with which you're doing, they did blood analysis. Right and if this would, for instance, be a, a tooling machine in an industrial company? Then, then, the manufacturers, they are really, really bastards.

They, they would say, yeah, we can upgrade this NT that we have built in, that we've embedded in our machine. We can upgrade this and use whatever Windows server 2016, but you know, If you want us to upgrade this, you basically have to buy a new machine. So here's your bill for 5 million.

And of course nobody does that. But because of that kind of effect, we still have a lot of machines out, out there for which we need to think about isolation, where application level firewalling and blah, blah, blah, to kind of keep them secure.

[00:24:43] **G Mark Hardy:** And do you see that also in the medical industry? Because once you have a device certified and it's a long process, and then you say, well, let's just upgrade the operating system. Why? Because, well, it's an old operating system, but it works. But it's old. But it works, but it has vulnerabilities. It aren't patched.

But it's not [00:25:00] connecting to anything other than the sensors. But, but, but, and then the problem is if it really comes down to what we were discussing earlier, was it risk acceptance. And what we as CISOs need to be able to do is go to executives and explain to them. Here is your situation and there's a certain amount of risk in your current environment.

Now, on one case, you can mitigate it by buying all new equipment, new operating systems, and pay a ton of money, but that's a new requirement to keep this thing patched. The alternative is, let's isolate this thing, make sure it stays isolated, that nobody can just plug into it with an RJ 45 cable and take over it

[00:25:35] **Michael Krausz:** one of the, one of the elements of the art of being a CISO is actually to be able to talk to management in their language and those CISOs who can't do that usually have a really miserable life because they don't feel understood and their management doesn't feel understood and this kind of gap, can't be bridged, so the most important class for a CISO actually, or for a CISO, is technically minded by Origin, is not the science [00:26:00] class.

It's a, it's a communications class, it's a class on accounting, it's a class on understanding, a balance sheet, understanding. C-level executive makes decisions, right? And once you can speak the language, you boost your own credibility and you're suddenly taken seriously. And then low and behold, you also get the budgets you want.

Because now your budgets are supported by arguments that your cfo, ceo, whoever you report to, hopefully a C level executive, but you know, that's no longer discussed anymore. That's kind of taken for granted, fortunately that they, they will be able to understand,

[00:26:32] **G Mark Hardy:** And that's a very good point because we were talking again before the show about the idea of secrets of a successful CISO, of course one of 'em you said is very paramount. It's gonna be communication skills, but also if you start out and you're an environment that's growing rapidly or it's a new security function and you don't inherit much of any staff, there's gotta be a way to effectively communicate that to management to say we need more people here. And oh by the way, what are the right [00:27:00] number of people and what are the right skill sets and and how do you do that?

[00:27:03] **Michael Krausz:** Okay. Well, thanks Mark. That's a very good question. So, basically we've come up with a model how to do that. So first of all, it starts with what is the basic principle of operation for a CISO department? Three functions. Governance, Consulting, Audit. Governance means being the owner of all the policies, negotiating them, discussing them, drafting them, blah, blah, blah.

Consulting means helping the rest of the organization understand security until they can do it by themselves. And audit means auditing the rest of the organization in regard to the level of adherence to the policies. So these are like the basic functions. So now the next very fundamental principle is really simple.

The number of people you need depends on what you need to do and how much of it you need to do. Because even if you have one task, but if you need to do it a hundred times per day, you still need five people to do it as a, as a simple example. Right? So let's talk [00:28:00] about what you need to do.

So, the ideal CISO department, first of all usually has an operations branch where they actually operate their own security systems, be it the SIEM, be it the SOC, be it anything else that, that IT cannot operate. They also deal with, security auditing on a technical level for operating systems, the network applications, blah, blah, blah.

So that's one thing. Then of course you need somebody who's able to write policies. You need an incident manager. You need somebody who can do business continuity. The data protection officer should actually report to the CISO because it's easier for a CISO to understand data protection than it is for data protection officer to understand technology.

Right. Then you'll need somebody for physical security and these, they should all be in your department. So that's basically kind of the what. And if we now look at how. Let's say about how you collate can collate the skill sets into headcounts. You will find [00:29:00] out, for instance, that an operating systems analyst can also do networking, but a networking analyst can't do databases.

A database analyst can do database operation layer, database application layer. But he won't do networking, for instance. Right? So if you look at all, I mean, we have very nice slides about this and presentations and blah, blah, but if you look about, if you look at this, the final answer on simply based on the skillsets that you need, is that the CISO department at least needs six people, period.

I will defend this in any court of law, six people, period. I remember, I remember being, having been appointed CISO for external CISO for industrial company, and I, I, I knocked on the door of, of the CEO who also represented the owner's family, and I told him, we are going to need eight people.

And he was like, what? And I said, we are going to need eight people. And he's like, well, we'll start with you and we'll give you one more . And then of course, five years later, we already had six people. [00:30:00] But you know, if you want headcount, it's a fight. You need to really make a good argument.

So first thing. Decisions sphere number one, what do you need to do? And this also depends largely on how the company is set up at that point in time. When the CISO department is created and it depends on what your business is and blah, blah. And now the second point is more or less easier to define.

Basically what you do as a freshly appointed CISO, first of all, you usually have to, deal with all the chaos and rectify all the infrastructure and stuff, right? But you also should have an Excel sheet where you write down, All your tasks that you do every day, and then you just, you make your list then you cross it off and then three months later you can actually tell your CFO or ceo, this is what I need to do, this is how it's going to develop.

This is the trend, and therefore I need more people because you're then, Facing your communication on facts, not on searches, a gut feeling or something you want. American managers, for instance, [00:31:00] American C levels are extremely suspicious of gut feelings. You can't approach them with a gut feeling.

You have to approach them with numbers. Right. And so creating a fact set of numbers by simply measuring what you do Yeah. Is a good starting part. Of course, you can anticipate that like, let me just bring up something here. When we started thinking about how to actually bring a system to, to determining staff numbers, it, it basically came from the fact that I've never seen a CISO department that wasn't understaffed.

And I've never seen an IT department that wasn't understaffed. Right. Usually, if I have a new project that's like consulting Secrets of the successful consultants, so to speak. When I have a new project and I work with a ciso, I always bring that topic up cause I know he will love me for it.

Right. So, in regard to the, what, so there's the operational aspect, taking running security systems. There's also, what I forgot before was, secure software development. That's an art, it takes a company, something between [00:32:00] one year to three years to, to redesign the development processes to actually be secure software development processes.

And in that phase, if you're working as a CSO for a SaaS company, for instance, or whatever, in a company producing software, Your first emphasis will not be on the network. It will be on making sure that development actually produces software that's secure and secure and doesn't expose your customers, right?

And then, you will find that you will have, for instance, 10 people in your software auditing department, but you might only have one person in the networking department. So, incident management policies, procedures, awareness building, usually with the CISO department, let me be a little brutal here.

The classical security analyst, who is a very, very strong nerd, is not the best person to do security awareness training. Cause the one doing it needs to be able to empathize and relate to people, not just systems. If we look at the different skill sets that are needed for a CISO department, first of all, your operations people need [00:33:00] to be good in technology.

Your secure development people need to be good in technology and programming. Your incident and breach manager, he needs to be able to design and follow processes. He needs to have investigative skills and he needs to be able to write reports, right? Another skill that is hardly found in IT, frankly speaking, Mark, one of the secrets of our success is that we haven't never found an IT department that does its documentation properly and we do it for them.

Because, we are the language people. We can write these documents and we enjoy writing these documents. Whereas, the typical system administrator is what I call documentation allergic. They don't like to document.

[00:33:40] **G Mark Hardy:** And it's also an important skill for people getting in the consulting world. I know like my son is a pen tester and I had hired him previously before he had a full-time job and we'd done a couple things and it's kinda interesting when you see your own case, like, wow, you actually write really well. Why didn't you do this back in high school? it's

[00:33:57] **Michael Krausz:** Exactly,

[00:33:58] **G Mark Hardy:** grade. It's like it [00:34:00] didn't matter back then, but now you get paid for it.

[00:34:02] **Michael Krausz:** Yeah. Let me just finish this train of thought here. for instance, the one in your CISO team who writes the policies and procedures and who does the awareness training? What, what's the primary skill needed? It's language and people skills. It's not technology.

The one who does project security, which is actually something ISO mandates. This is a person who needs to have tech and people skills because he needs to understand the technology, but we also needs to tell people what to do. Now, the data protection officer, of course, is is a legal person usually, but ideally it's somebody who has a good understanding of the technology background of your company.

And the physical security officer basically has technical knowledge, but you know, restricted to physical security systems and also needs to be good in project management because, if you have multiple sites all over the world, getting them all secured from a physical point of view is a huge challenge.

And then of course it depends. For the CISO it basically depends what he was hired for, so a CISO of course has to have leadership skills, business technology skills, [00:35:00] and whatever. You do, I mean, I basically, I, I distinguish between two. Types of CISOs. I call them the techies and the orgies.

The techies are those who love technology and want to play around with technology. And the orgies are those who love organization, who love processes, people, and you will find. I, I bet, I bet you one, one Saha cake. You know that the first CISO in any company is always a techie because usually the company starts out with a huge pile of, let's call it technical debt in instead of, those words that you've, for, forbid me to say on, on the podcast, right?

So, the company starts with a huge pile of technical debt that needs to be work off. And of course, a technical CISO is the best one to do this. But you know, at one point this technical CISO will reach the glass ceiling of having the glass ceiling, of knowing how a budget is made, how to read a balance sheet, how to [00:36:00] communicate facts to C levels, how to align strategically.

Right. I've seen technical CS fired because they insisted on a specific type of firewall to buy. This person insisted on that, he felt insecure when having to even think about another type of firewall. And such a person is simply not suitable for the leadership position because, in a leadership position, your personal feelings about the technology simply don't count.

You have to be more rational about this. What about cost? What about ease of use? What about maintenance costs? What about blah, blah, blah, blah, blah, right? So you can't be, frankly speaking in a leader position. You can't be a nerd. As a specialist, you can, and you're very well appreciated there.

All good CISO departments love their nerds and and they pamper them, but in the position itself, you can't be. Then at one point that CISO either manages to break through the glass ceiling, out of, for instance, by getting training. Or he simply leaves because he gets [00:37:00] frustrated.

If you have to have the same discussion with your manager, cause they don't give you enough budget, because actually you can't communicate why you need that budget over and over and over again. At one point you just leave and then you know, the new C actually finds something that is usually pretty well established. And that CISO is usually an orgy because his challenges are no longer technological. They are rather organizational, getting the processes done, getting the procedures done, or for instance, getting the company ISO certified. Getting a company ISO certified is not a technological project. It's a cross-section project across the whole company. Right? So basically, like, like in this kind of systematics, there are three steps. One, what do we have to do and how much of. Two, what are the skill sets that we need and how can you combine these skill sets to minimize the number of FTEs. You wouldn't want to start with 100 people. You'll never do, you start with one, three, maybe five, right?

And and the third thing is after you've done that, the, from these [00:38:00] two steps, the minimum number will follow. And it's usually not less than six. So, in this particular case that we just looked at this year so actually a friend of mine who I worked with five years ago, he started six years ago in his company, He started with zero. He was alone. And the first project that he got wasn't even a security project. It was an IT ERP implementation project, but he managed to go from zero to 45 people within five years. And how do you do that? One? Never undermine your credibility. Always be rational. Accept that some things can be done and other things can't be done.

Number two. Always lead all arguments in terms of risk, right? Make the risk transparent, and then you can basically withdraw yourself and say, okay, you are the C level. You decide what to do with the risk. And in his situation it was even worse because he had a lot of country subsidiaries who had complete freedom.[00:39:00]

It's also like a nice difference. In America, companies tend to be very hierarchical and if the headquarters says something, all the subsidiaries do it, like in this particular company. And more or less it's also European, European kind of mentality. They, the subsidiaries usually can do what they want.

Which for security is bad. For business it's even good because you can be more flexible in regard to the market you serve. But from a security perspective, it's bad. In his company they had seven different malware scanners. What for, buy one and you save on license costs.

Why seven? Because everybody made their own decisions. So the biggest problem for him was actually to get the subsidiaries to cooperate. And he did this in a very, very clever way by, in his first year as a full CISO, just doing a risk analysis. And the risk analysis showed exactly what he knew right from the start, which is secret number three.

Always be one step ahead, because what did it show? It showed they don't cooperate. And with proof of them not cooperating, he could approach the board and say, this is [00:40:00] no way to continue. We need to change some things here. And this is how step by step with every technology he, they introduced from, from doing simple vulnerability management and penetration testing to risk analysis, to awareness trainings.

He always did it in a way where first of all, he told the subsidiaries, do what you want, but this is what we suggest. Full well knowing that they simply will fail because if they don't have the knowledge, what else is the outcome? So, and in every cycle, in every couple of years with this more strategic projects, they simply failed.

Got back to him and said, what do we do now? And he was like, Hmm, here it is. What we, we need to do. . And because of that, because of this psychology, his credibility with the board always got stronger, stronger, stronger and stronger.

And this is why after five years you end up from zero to 45 people because you never jeopardize your credibility with the board. However, there's one catch here. I mean, I do have to say, this is my company of about 10,000. [00:41:00] And of course, this is a company with a very, very stable business model.

And this is why you could actually play such a, let's call it game, because you need to have the stamina in a very fast moving business. You can't just wait a year for the subsidiaries to F it up. sorry, couldn't contain myself. Hope that's borderline. Okay.

[00:41:20] **G Mark Hardy:** No problem.

[00:41:21] **Michael Krausz:** So you can't wait, in, in a fast moving business, you can't wait for the subsidiaries to fail full well, knowing that they will fail.

You would be a little more proactive and a little bit more forceful in, getting things right from the start. But in this particular setup, which I mean for big companies, it's actually rather the same. A big company doesn't move fast. they never do. So in that kind of setup, you could pretty well take the time to just wait until those who are you are supposed to consult in this until their own way simply don't work.

And then you can draw your card out of your sleeve and say, this is how we do it. And none of his strategic initiatives, none ever failed of his own. [00:42:00] Right? Because he always kind of reacted to, very cleverly to something that he had suggested, which the others didn't pickup

[00:42:08] **G Mark Hardy:** Interesting. Yeah I see we're out of time. We, we ran all the way to the end of the clock and then some, but absolutely worthwhile. I mean, kind of a quick recap. I know we were talking early. About ISO and the the importance that between policy, practice and proof, and then we looked at the role of the CISO looking at governance, consulting, and audit.

The types of CISOs could be technical or techy versus an organizational orgy as you called it, and then being able to go ahead and staff your people, being able to identify what needs to be done. How much of it needs to be done? Who are the people who needs to do that? Tracking the work that has to happen, and then being able to use that as hard justification.

And then ultimately, when you're dealing with trying to grow your organization, it's making yourself credible to the board and not letting go of that credibility. And I think those are all tremendously great insights for our listeners. And I, and I [00:43:00] thank you very, very much for your time and for your expertise.

And so any parting thoughts before we sign off?

[00:43:08] **Michael Krausz:** Not really. I feel a little exhausted now

[00:43:11] **G Mark Hardy:** So anyway yeah, let's just wrap it up. So this is CISO Tradecraft, your host, G Mark Hardy. It's been a privilege to be here with Michael Krausz. He's from ISC Co over in the Austria. You can look him up if you will Google him or he is on LinkedIn. And if you like our show, please follow us on LinkedIn.

We put out more than just shows and in addition to that make sure you give us like a thumbs up or a five star in your favorite podcast platform so other people can find us. Thank you very much for listening and until the next time, stay safe out there.