#227 - The 30 Year CISO Evolution

[00:00:00] **G Mark Hardy:** From the very first CISO, today's Threat Hunting Boardroom advisor, the role has come a long way. Today, we're gonna walk through the chemo and it shaped our CISO careers. And if you're leading security today, you're standing on the shoulders of giants and maybe a few firewalls.

Hello, and welcome to another episode of CISO 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, your host and fellow CISO, and today we're gonna dive into the timeline of our profession, from the humble beginnings to the relevance we have today in the boardroom.

And whether you're new to the CISO job or a veteran like I am, this episode is your time capsule of how we got here and where we're going. Let's start with a man who, [00:01:00] start it all. Steve Katz. Steve Katz before he became the World's Chief Information Security Officer of the CISO at Citibank in 1994, this gentleman had already built a robust career in both information technology and information security.

So he had a real strong foundation for this historic role. So if you're wondering like, how do you pick like serial number one, he was vice president of technology and risk management at JP Morgan before he joined Citibank. He was responsible for managing technology risk. worked early strategies for safeguarding financial systems.

Gave him direct experience in integrating security with large scale business ops. And then, although the role of a CISO didn yet exist, he was already focusing on security and risk and things that are core to the discipline. Access controls, secure network architectures, incident response processes, and a lot of this work had an emphasis on governance and how do we align our security with our business objectives

plus he had built a reputation for a business and technology [00:02:00] integration. He was able to translate technical risk into business language. You probably heard that on the show a lot. And the known for bridging the gap between the IT and a business, which was really important when Citibank was trying to create a security leadership role that would report to and then appeal to the executive suite. Now, in 1994, Citibank had a significant cyber incident involving Russian hackers, no surprise, infiltrating their systems. And at that

time, information security was largely an ad hoc responsibility. It was part of what you did as a collateral duty, as an IT administrator.

There really wasn't a cohesive strategy. There wasn't a governance model, really no executive oversight dedicated to protecting digital assets. Now I was doing IT security consulting back then. I had started my first business back in 1988 and I was focusing on doing that very niche piece of the IT job that was security.

And I can tell you in my early days, it was a little bit like hand to mouth where you'd go ahead and you'd get a contract, you'd work the job, you'd get paid, and then [00:03:00] take all that money and you burn it up trying to find the next customer and things such as that. Well that early Pioneer stage gave way to a little bit more of a professionalism because Citi had recognized having an centralized executive level security oversight with someone like Steve Katz.

He's got technical understanding, risk management experience, communication skills. Hey, what a winner. So he became the first chief information security officer. Now, what was the first job? Build an organizational wide cybersecurity program that's gonna report directly to higher levels of leadership. Now, he approached this with some vision.

It was just a technical hurdle. He looked at it as a risk issue, had business implications, frameworks for risk assessment, collaboration across departments, and defining what cyber governance could look like. So it really wasn't just a new job title, it was beginning of a new type of leadership, someone who could bridge business technology and security and bring it together.

Now, as the [00:04:00] 1990s progressed into the early two thousands, we had the rise of security certifications. ISC2 launched the CISSP certified Information System and Security Professional back in 1994. Covered at the time, 10 domains, and now we got eight that range from cryptography, security, architecture, legal consideration, et cetera.

The idea was to set a foundational basis for cybersecurity leadership. Now, only 46 people got CISSP the first year, but by the time the new millennium came around, it was almost a 3000 and I, remember. When the founder of that kind of came to me and he said, Hey, Mark, Hal Tipton, you oughta get the CISSP.

It'll be good for you. And I, it should been 94 or 95, so I probably could have had a two digit CISSP number, but I didn't get the vision. I didn't wait, waited

until 2000. So yes, my CISSP is over 25 years old and probably the people who are still practicing it might be in the top [00:05:00] couple hundred survivors.

But so what? Who cares? The idea was it started the concept. Of a certification is a testing what you knew. And in 2002, ISACA came out with a certified information security manager credential, and I was more focused on strategic alignment risk management. Great. If you're aspiring a CISO, I actually applied for under their grandfather rules, the fact I was already existing practitioner.

Could have been grandfathered into CISSP and I'm thinking like, I didn't get the vision. this time I get corrected. It's yeah, I'm gonna hop on board. That. And having that CISM, I continued to pay those dues and had been doing so for, again, about 25 years as SANS introduced the GSLC, the Global Security Leader certification a couple years later.

In response to the growing recognition that cybersecurity leadership needed more than technical expertise, you had to have strategic oversight. Policy, governance, risk management, and the ability to communicate effectively with executive leadership. Now, SANS has been known and still is [00:06:00] known for their excellent technical courseware, GSEC, GCIH, being able to culminate in the GSE and for my fellow sans instructors, when I used to work there, having a number below 100 was a big deal.

Having a one of the first global security experts. But Stephen Northcutt, started teaching in management 512. Wrote it, taught it full disclosure. I taught that course, for about 10 years at SANS and really loved it. I thought the content was awesome. It had things like governance, risk management, security frameworks, policy development, business continuity, disaster recovery, incident response, legal issues, budgets, security awareness programs.

All these things are part of the portfolio of what we do as a cybersecurity professional today. These certs filled a major gap because HR departments could now qualify a candidate with an objective standard, because there's a lot of opportunity that was not yet there in the university world. You couldn't get a degree in cybersecurity can now, [00:07:00] but in the early days, it really wasn't out there.

When I went through and did my computer science degree, hey, it was with punch cards. I guess I'm showing my age a little bit. In any case, when I had a chance to work as an adjunct professor. It turned out that the approval process for curriculum change took a long time, and as a result, a certification program

that could make changes two and three times a year could really get inside the decision cycle.

For those of us who understand the term, the OODA loop, the observe, orient, decide, and act of the universities, and so certs became the currency of the realm in cybersecurity more so than the degrees. Now, it provided credibility. Then what happened is we started to see all this training taking place is say sans, which quantitated all the way back to 1989.

Hard to believe that I started a company a year before them, but of course they're now probably a nine figure business, doing quite well and adding all kinds of value to the community. They [00:08:00] had all of these analysts, defenders incident responses, as well as people who want to work their way up into the security leadership positions.

EC council launched a certified ethical hacker, the CEH. It would take offensive security turn into a legitimate career path, and now with offensive security, you have practical lab-based exams. They're really gonna push your candidates to prove real world skills. For CISOs, this is a transformational development.

You could hire team members that had verifiable specialized skill sets, and then you yourself could pursue leadership training that would actually align with your operational reality. sometime in the two thousands we got all this regulatory wake up call after Enron world. Carl Sarbanes XI Act was passed in 2002, and that required publicly traded companies to establish strong internal controls over financial reporting.

for CISOs. This now all of a sudden means that you might have a seat [00:09:00] at the audit table 'cause it controls change management data integrity. These are no longer optional, these are mandated. At the same time. The healthcare section saw HIPAA's security rule finally go into effect in 2005, although it had been around for a number of years.

But there we had to have administrative, technical and physical safeguards to protect. Patient data. Then the retail world was introduced to PCI-DSS version 1.0 came out in December of 2004, and that standardized how payment card data should be handled. See, these compliance regimes created a whole new era of accountability.

CISOs had to evolve their roles from being a protector of systems to interpreting regulation, ensuring that the security controls aligned with the legal obligations. It was really the beginning of the CISO's, dual identity technical expert and

compliance strategist. As we roll into the two thousands, we also find out that well, money gets involved.

I remember sitting through the.com crash back in March of 2000. [00:10:00] Sounds a little bit like last weekend. And for those of us who are listening to this show live. but here in April of 2025, we just had the interesting back to back days. after the.com market crashed. It didn't mean that technology was wiped out.

It means you shouldn't simply couldn't just start a business saying, it's gonna be on the internet and we don't know how we're gonna make money and we're gonna lose money on every customer, but we'll make it up on volume. And that was the mentality back there in 1999, 2000, we got serious about it.

And so we had companies like e-sentire . I used to be on their advisory board, wished I stuck around. They're now a, unicorn. FireEye started in 2004. Palo Alto Networks in 05. Tanium in 07, Zscaler in 08 and CrowdStrike as late as 2021 and, or I'm sorry, 2011. And investors poured billions into cyber startups.

and now all of a sudden the CISOs have access to a whole bunch of innovative tools. But, [00:11:00] With great choice comes great responsibility. Now, as a CISO, you're the gatekeeper and an influencer in this new vendor economy. You have to evaluate new solutions, not just for the effectiveness of the technology, but does it align with the enterprise architecture?

Does it have the operational capacity to meet your requirements? Can does it conform with your risk appetite in terms of what it's gonna do for you? And actually, is this company still gonna be around in a couple years? See, a smart CISO could use this moment to reshape their tech stacks, and if you're thinking forward, you can even partner with vendors, co-develop features, shape roadmaps, and now you're not just a protector anymore, you're a market influencer.

I had the privilege to work for a couple years in the CISO board with a company called Red Canary. We've had their founder on the show, and what they did is they brought in several, chief Information security officers who are customers. And said, let us show you our roadmap. Let us hear back from you as customers what you need so we can build the tools and the capabilities you [00:12:00] want.

I thought that was brilliant. I still have monthly calls with my Red Canary success rep. No, this is not a paid ad. This is just happy customer talking, and I

don't know why nobody else does that. They're the only company that have a regular call with once a month. So if you're. Cybersecurity company and you want to increase your stickiness to your customers and have them become raving fans.

Call 'em once a month. Now, over time, we found out that cybersecurity turned out not to be just the interest of companies, but governments as far back as 1998. 1999 was Moonlight Maze. Suspect suspected Russian government actors, targeting US Department of Defense, Department of Energy, NASA , even private defense contractors.

It was really the first publicly known state-sponsored cyber espionage campaign and involved access to highly sensitive US networks. Focusing mostly on the government, exfiltrating vast quantities of data, including classified information and research. [00:13:00] It demonstrated that cyber attacks could be used for long-term strategic espionage.

It prompted the US to begin seriously considering cybersecurity as a national security concern. Oh, cyber command didn't come around for another decade or so. Titan Rain, which is believed to be Chinese military hackers, probably unit 6 1 3 9 8. APT one, was targeting a Lockheed Martin Sandia National Laboratories, nasa, army Information Systems.

And really those were coordinated attacks going after defense contractors, government agencies to steal sensitive military and aerospace data. And it demonstrated a very high level of sophistication and persist by the attackers, which is where we got the A PT, the P there. it's really one of the first acknowledged.

Large scale economic and military cyber espionage campaigns, and also marked China as a rising cyber power and brought attention to the intellectual theft of property. So almost 20 years ago now, think how far [00:14:00] China has come in that capability. By 2009, 2010, operation Aurora, Chinese State sponsored hackers, had targeted Google, Adobe Juniper, Morgan Stanley.

20 other companies and they exploited some zero day volume and Internet Explorer to gain access to internal systems and email accounts. Now, Google went ahead and exposed that attack publicly in 2010. It's a pretty bold move at the time. Now, of course, zero day publications and being able to have the announcement of, hey, something is a breach, or more precisely something has a evolved, it's been reported to the vendor, sorry, vendor.

You got 30 days or 60 days to fix it, and then we're going live with it. Created some accountability, some transparency and assertiveness on Google's part in terms of their, response for it. But it's also a wake up call to the state sponsored corporate espionage and, Just one more for fun.

STUXNET, which is discovered in 2010, and the perpetrators have been ascribed to [00:15:00] United States and Israel, though neither country has ever said, yeah, we did it. It's a suspected likely because their target was the Iranian nuclear facilities, especially at Natanz, and it was really the first known offensive cyber weapon. And it really began cyber warfare as a strategic military tool. And for those who aren't familiar with the history of Stuxnet, it was basically sabotaging Ute on's uranium enrichment process, the uranium hexa fluoride that they would go through and isolate. And the Siemens programmable logic controllers, were targeted basically SCADA systems.

And it showed that you could actually cause physical destructions of things through a cyber attack. It really did bring up a huge question of, how do we go ahead and keep this genie in the bottle if we can? Oh, by the way, the question I used to ask is, would you send your sons and daughter in the war, kinetic war against an attacker who launched a cyber attack against you, but didn't put any bombs or missiles or guns, or anything else?

It's an interesting question that [00:16:00] we haven't yet figured out yet. in 2014, Sony Pictures got hit with a significant breach. It was attributed to North Korean state actors. they had, film out, I think it was called the Interview, that was not positive with regard to the beloved leader of the Democratic People's Republic of Korea.

And so therefore, the US company got hit, which basically said, no industry safe, no company safe, and the motivations may not just be financial. And then the next year, OPM breach, I remember that one Chinese actors exfiltrated the personal data of over 21 million. Government employees, current, former, and then all their contacts that they had, which is all about security clearance.

Now, that is a massive win, if you will, for China, because if you know everybody who's got a security clearance in the United States, some of these people are still gonna be around 20, 30 years from now. They're early in their careers. In addition, we had seen future hacks that go against the. Healthcare databases [00:17:00] that companies that provided healthcare insurance for federal employees and then credit reporting bureaus put the pieces together.

What can you do? This particular person is a high level clearance and it indicates that they have some health issues that aren't being addressed by the insurance companies. 'cause insurance companies are pushing back and, oh yeah, they've got some financial problems. What a wonderful target. To go and try to recruit them or to go ahead and put a little bit of leverage on them, with regard to.

Turning people into, spies or whatever. we, find out that the cyber stuff has really gone very high order. we now gotta think of the geopolitical actors in our threat models. It's not just stopping criminals, it's gotta counter espionage, sabotage, psychological operations. And now the boardrooms are starting to sit up and take notice, who might want to target us and why?

And now threat intelligence became a big industry and. It's required capabilities, not just a luxury. And then by the time I got to [00:18:00] what, 2017 was WannaCry NotPetya, this is Destructive Malware. if you remember WannaCry, this came out in May of 2017 and they were able to spread through some stolen tools that were originated at the National Security Agency.

A group known as a Shadow brokers went ahead and leaked it in something called Eternal Blue, which would take advantage of a weakness in Microsoft's SMB protocol. So this self propagating ransomware would go sideways. It would work without user interaction, zero click and then you could go ahead and demand Bitcoin for encrypted files In 2017, a lot of people didn't know how to get Bitcoin, and I like to say an executive trying to buy Bitcoin is like a grandmother trying to buy heroin.

They don't know where to begin. Plus it was a lot cheaper back then, but the impact was over 230,000 computers, over 150 countries, and it spread within hours. The UK National Health Service was hit, FedEx was hit Renault, $40 billion [00:19:00] in, global damages, and they figured it was probably the Lazarus group.

Democratic People's Republic of North Korea, who have, set some records lately in their ability to go ahead and get billions of dollars through cyber crime. Not Petya came out to you, but it's just a month later. It looked like ransomware, and when it first came out, when I heard they had ransomware out there and it wasn't working correctly, and it seemed to have a Russian origin, I'm thinking, yeah, there's gonna be a bullet administered in Moscow because someone has broken this sacred oath among ransomware operators.

Think about it. If there's an industry on ransomware, and it's well known that if you get ransomware and you pay the ransom, you get your files back. Then what's gonna happen the next time you get ransomware? just pay it and we'll get our files back. But then somebody comes along and says, Hey, you pay it and we don't give you your files back.

You're breaking that model and all of a sudden people are gonna stop paying. it turned out. It wasn't ransomware, it was a wiper. It just was [00:20:00] masquerading as ransomware because they all went to the same address. So you couldn't even sort out who was who in the zoo in terms of people who wanted to give you some Bitcoin.

It went through infected software doc, updates, from Meoc, Ukrainian accounting tool. Also used Eternal Blue, eternal Romance, mask, what a $300 million. Hit from that America sne, FedEx, over $10 billion. Total damage. This is collateral damage. Not really the primary target. The primary target was Ukraine.

This is 2017. We've seen Russia and Ukraine not getting along all that well for quite a few years now, and, was believed to be GRU and it ended up with a global fallout. So the old assumptions were, Hey, your perimeter defense is fine, but if you have a patch management failure. There's something that's not up to date, and then lateral movement is possible without your enterprise.

It's a massive consequence, almost existential to your company. [00:21:00] So now resilience became really key. Business continuity planning, disaster recovery, cyber insurance. We had to take a look at that. And now as a CISO, you have to become a crisis manager. And now cyber resilience is a board level concern. by 2018 we have GDPR, the General Data Protection Regulation.

It went into effect 99 different paragraphs and you have trouble sleeping. Go ahead and read GDPR all the way through. I have, I didn't fall asleep though 'cause that's what we do for a living and some of us find it interesting, but it basically forced companies worldwide to reevaluate how you collect, store and process personal data.

It empowers data subjects, be IE people, European citizens with the rights to access, rectify and delete their information. And as a CISO, this is a paradigm shift 'cause security controls now have to align with privacy principles, encryption. Pseudo nominization say that fast five times and data minimization are no longer best practices.

These are [00:22:00] regulatory requirements. You gotta do it. And then a 72 hour breach notice, oh my goodness, how are we gonna do it that fast? Of course, today we see things that have a lot shorter. Fuses on there, but there's a huge pressure on detect and respond capabilities, and then it's also gonna elevate the importance of cross-functional partnerships.

You gotta work with the privacy officers, the legal teams, and the data stewards who are out there. for those of us who, lived through the Great Pandemic and most of us alive here, I think have, and it created what the largest remote workforce experiment in history, starting in early 2020.

Practically overnight, organizations had to support entire workforces outside the corporate. Perimeter, our VPNs maxed out and we couldn't handle it. The home networks became attack surfaces. Personal devices got pressed into service because we didn't have them. And so they didn't have copper controls on it.

Family members were using it. You're out and playing Minecraft in the evening and dad's going ahead and working on stuff during the day, and then mom's working on her job on the afternoon, and who knows what the [00:23:00] kids have put on this thing. And so now, as a CISO, you have to have agility. You have to be able to respond to these changing environmental conditions.

You can't sacrifice security. Where's your new perimeter? It's identity. And now we have to go to zero trust models and endpoint detection and response and CASBs and cloud security platforms. And now all of a sudden you have to accelerate your security programs and all that technical debt comes due. And it's also really a cultural inflection point because if you succeeded as a CISO in making your organization.

Go through this. You became a trusted advisor to the business. You weren't just a policy enforcer, 'cause you could do transformation while maintaining trust. I remember in early 2020 when I had just finished completing writing an incident response plan on disaster recovery plans for the organization.

And then my client had said, Hey, could you write a pandemic response plan just in case? hey, I [00:24:00] already had the template, so you changed disaster to pandemic global search and replace a little bit more than that, but not too much different than people can't get to the office because of a massive snowfall or earthquake or flood or fire or building shut down or anything else that would keep people outta the office.

It was a much, the model was built around and then we tested it, told everybody, bring all your equipment home, your phone and your laptop and your chargers on a Wednesday, work from home. Nobody ever done that before in the history of the company. I always came to work Monday through Friday. On Thursday, we all come back in the office.

We sort out notes and things like that. What work, what doing. Okay? We said, okay, Friday, so Thursday night, take your stuff home with you again. Work from home on Friday. Have your chargers, your paperwork, your laptop, and we'll talk about on Monday. over the weekend, Washington DC shut down and they stayed shut down for 66 weeks.

We had zero interruptions in the business. Everything kept rolling. Why? Because it got lucky because we had tested this plan literally the day before Everything went down [00:25:00] and we had all the bugs worked out, and as a result, other companies scrambling, forgotten activity. scramble, We did just great.

Let's look about today. What challenges do we face? As a CISO, you gotta deal with risk. We deal with resilience, we gotta deal with reporting. you gotta be a technologist, a communicator, a strategist. Regulations are only going up more and more. Now, the SEC requires your public companies to disclose material cyber incidents within four days.

I gotta be fluent in disclosure language and materiality assessments. Boards say your metrics have to tie cyber risk to the business outcomes. That can't be just focused on it. We've gone from technical dashboards. To business aligned risk scoring, and we've also got personal liability. Had a chance to spend some time with Tim Brown several weeks ago.

This poor gentleman has been, standing in the gap, if you will, for our CISOs, community dealing with an a tremendous amount of time. If you don't know about 'em, I'll get 'em on the show you've already agreed to, and I'd love to have him [00:26:00] tell your story about that kind of a precautionary tale of what could possibly go wrong when you don't think you're doing anything wrong.

but, here's the thing. With these lawsuits, regulatory actions, now we're 10 potentially in the target, and the good news is, that if organizations recognize the strategic value of cybersecurity, then maybe the CISO's gonna be protected by the eras and emissions, the executive and the directors and officers policies and things like that.

The Professional Association of CISOs, whom I had on the show about a month ago. Join that and work with the PAC. You can get the liability insurance for that and things such as that. And so I'm still going through, I'm a little bit late on my paperwork, but, going through there for their accreditation. But now the modern CISO has influenced 'cause you're shaping digital trust so well, where does that leave us?

Calling back 1994 from Steve Cass to today, where our CISOs communicate risk. We face the boards. We're considered executives, although I still argue in a lot of places, it's a little C for our CISO, [00:27:00] but the CISO role has transformed dramatically. We've got compliance, we've got training, we've got vendors and all that assortment of stuff that we have to manage.

Cyber warfare, privacy, law, compliance requirements, all this chaos. We have to turn into clarity. If we've done so effectively, we have earned our seat at the grownups table, so to speak, to be able to communicate with and help senior executives make decisions. So what's going forward to us? AI driven threats, quantum vulnerabilities, reporting for ESG and maybe even a greater expectation to build a secure.

Digital ecosystems, plus the concern that comes with the warfare that's going on around the world, and can that extend out more into the cyber world? history shows that we adopt and we evolve and we lead. So for our CSOs out there, thank you for listening to CISO Tradecraft. I hope you found this interesting and a little bit, [00:28:00] revealing about the background.

if you love CISO Tradecraft, make sure you're subscribing to us. Follow us on. YouTube like us there. Listen to us, our favorite podcast channel, tell other people where they hear about it, and then give us some feedback. We're on LinkedIn. We got a lot more than just podcasts. We'll go ahead and have a Substack newsletter.

We have little out cakes and shorts and things that we put out there. Help us help you in your career to do better. So this is your host, G Mark Hardy. Thank you for the opportunity to spend the time with you. until next time, stay safe out there.