#215 - CISO Predictions for 2025

[00:00:00] **G Mark Hardy:** 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. I'm your host for today, and we're going to be talking about top 10 predictions for 2025. What is it that we might be able to expect in the future?

And maybe we'll come back in a year and see how well we did.

[00:00:33] **G Mark Hardy:** Hey, a couple of little insights for you, by the way, This Wednesday, if you need CPEs, I'm doing a full day course with ISACA. It's the 21st annual day with G Mark. It's been great. I've been working on the Central Maryland chapter and you can get your CPEs for pretty much any cybersecurity certification.

If you want more information, go to ISACA.CISOTradecraft.Com to register, but don't wait for too long [00:01:00] because it's filled up the last couple of years and the, prices are quite reasonable. Also, don't forget about CruiseCon coming up in February. CruiseCon.com. I'll be there and there's an opportunity to go out there for an executive cybersecurity cruise, get away from the cold and everything else, and spend some time networking with other fellow professionals.

Okay, so what can we potentially expect for 2025? The first one we think is that AI influencers are going to become normalized. Now, what do we mean by that? You've probably heard the famous song that video killed the radio star, and it's a famous tune that dates way back to the fact that, with the advent of video, unattractive singers has a limited lifespan.

It just didn't happen in the music industry. It happens in news channels. It You basically have to be a model to land a job as a weatherman or weatherwoman or whatever role that they have today in the TV shows. And we saw that happen in magazines, men's health for years, they photoshopped our ideal of what the [00:02:00] ideal body would look like.

They've done the same thing for women's magazines, creating some unhealthy habits for people trying to say, I have to look like this impossibly skinny person. I remember reading somewhere that said if Barbie were a real person she would have an 18 inch waist and a 39 inch inseam or something goofy like that. In any case, these technologies that can create optimized photos of people are only getting better.

We're seeing the emergence of AI influencers. Now, if you haven't heard the term, here's what we're talking about. Imagine a highly attractive model that captures your attention. To make it even better, this model could talk about. anything that the talk track puts into his or her dialogue. So ChatGPT can write an amazing article about the top seven new use cases for artificial intelligence security.

The dialogue could then be given by a very attractive model that was created. Basically digitally, there is no person that corresponds to that and the quality of these digital AI influencers has gotten to the point where I can be able to tell who's real and who's fake. So would you rather [00:03:00] watch cyber security awareness training from a model that puts Scarlett Johansson to shame or you want to hear it from some old white guy like me, who like, man, don't look at all that exciting.

So it's going to be an interesting future for what becomes popular. I'm hoping I don't get replaced by AI. We'll find out. It might even end up with a dystopian future like circuits from 2009 old Bruce Willis movie and in that future Everybody hides what they really look like because well, they're embarrassed by their human flaws All right, number two branding will rely on production quality a lot of folks in ranking content It's gonna be hard to differentiate cyber security guidance There's a lot of stuff out there.

Not all of it is good. Not all of it is relevant. Not all of it is even right. Because of this, we think there are going to be three things that are going to make influencers stick out. First, they have to have good content. Ideally good technical content. Now think of the content here on CISO Tradecraft.

It's not fluff. It's prescriptive. It's actionable guidance that you can [00:04:00] follow to improve your career and to help the people around you. Now, secondly, not only do you have to have good content, you need great communication skills. Nobody wants to listen to somebody who sounds like Ben Stein as the teacher in Ferris Bueller's Day Off.

Bueller, Bueller, remember that one. And third, There's a lot of smart CISOs out there who are sharing their thoughts on formats like YouTube. And so the last differentiator is going to be production quality. We really think 2025 is a year that CISOs will need to learn how to edit movies to create content that attracts.

Using clips, captions, music, special effects will now become the norm. You want your content to stand out. If you can do that, you can build a brand. yeah, I just am in the process of returning a new 4k camera. It was really cool. It had AI in it, I could hold up my hand to make it zoom, zoom, zoom, like that.

Unfortunately, it didn't play well with my other devices. And when I plugged it in to go ahead and try to record it, it overrode the use of my studio microphone, [00:05:00] and it sounded terrible. And also my USB light flutter and it did three or four other things. I'm just thinking I wanted better video, but so what it's me in any case, I'm hoping that the content of what I'm putting out, but that's going to be a differentiator is how professional your stuff looks and sounds.

Number three, collaboration between Google and Apple. Now, given the recent events from Salt Typhoon, stealing SMS messages from telecom providers, we predict that Congress is going to force major manufacturers like Google and Apple to create standards that are going to improve security. For example, why can't they both adopt the best SMS standard that allows encryption of messages across platforms?

Because if you're in iPhone to iPhone that can stay encrypted and I can go ahead and use other tools. But when I have to bridge from an Apple to an Android, it's got to go through an intermediate step. That's where it's decrypted. you're only going to see that at the telecoms. What was Salt Typhoon all about?

Adversaries in our telecom network. [00:06:00] Okay. So let's try to go ahead and remove that point of weakness, have a standard, and the alternatives are going to just continue to balkanize. And we have WhatsApp and Signal and all the other tools. I've got four or five different messaging apps there and I got to choose them based upon the individual with whom I am communicating.

And it may not always be the best one. By the way, my personal preference, if you ever want to connect to me, Signal. Number four. Application Security and Vulnerability Management Consolidation. Now, Team8 put out a paper called Fixing Application Security, which highlighted the average cost of application security tools can easily exceed 650, 000 per tool when you're all said and done.

Now, this arises from the cost of developers, which is going to be the majority of it, could easily come up to 500, 000 when you have salary and benefits and overhead and things such as that. And then the vendor licensing costs, which might be a bigger 200, 000 in relative to The labor costs, but [00:07:00] you got six different application security tools like vulnerability management, SAST, DAST, SCA, secret scanning, cloud security, that investment will add up.

It could be up to 4 million or even more. It's a lot of money for application security and vulnerability management. Now we expect to see a lot of consolidation of tools in this space. To a best of suite approach. For example, if you had one ASPM tool, one modern CSPM tool and one attack surface management tool, you might consolidate from 14 system administrators down to six while also reducing your licensing costs.

You could lower your costs from about 4. 7 million, all told to about 2. 1 million. There's a paper that we'll go ahead and put in the show notes. We have a lot more detail. It's a very compelling read. And for example, you take your SAST, your SCA, secret scanning, and custom single pane of glass, and put that all in your ASPM tool.

Take your vulnerability management and cloud security and put it in a modern CSPM tool. And then your DAST will be an attack [00:08:00] surface management tool. Take a look at it if you have to look at it. By the way, we're not talking about getting rid of people. We all have had a recent episode about What's really going on in the cybersecurity labor market, and we're advertising there's hundreds of thousands, if not millions, of jobs that are available, yet you talk to people who are experienced cybersecurity professionals who are getting laid off?

Barely recently. Other people trying to break into the career and not doing very well. So if you are facing that frustration, back up a few episodes, listen to what we talked about and maybe you'll find out some insights from there. Number five, Models Committees. Our next prediction is use of AI models and committees.

AI isn't something that's cleanly falls just under CISOs. Instead, we predict the creation of a new committee and large companies. Probably one step below the risk committee. It'll be known as a models committee. And look at the models used by data scientists and developers. And you can think of this as a risk committee that's been optimized to provide prescriptive feedback to [00:09:00] developers in what can and can't be used.

And we expect the models committee to consist of folks from compliance, cyber, and privacy. How about number six? Formalization of the CISO role. We're hearing more rumblings of the need for CISO role, just as other professionals have done it. Lawyers, accountants, doctors, we think this is going to take off this year.

Now examples will include the Professional Organization of CISOs or PAC. I know you can find their website at the CISO, spell that out, dot O R G. And this organization is focused on creating accreditation, code of ethics, partnerships to enable private reliability. Private liability insurance for CISOs.

Yeah, sometimes we need private reliability as well, and it's likely lobbyist groups. I think it's interesting about the private liability insurance. I was on a call yesterday with an attorney who was talking about all the potential issues that as CISOs, we need to concern ourselves with. And with respect to those comments, the idea is that if you work as a full time CISO, you should have something in your [00:10:00] contract, something that provides you with the, not only the errors and omissions, but also the protection.

from, directors and officers, DNO insurance. And you want to make sure that they're not going to just throw you under the bus. Now, in some cases, and this was an interesting conversation that he mentioned, you might be better off just to get fired. Why? Cause you don't want to spend the next six to 12 months of your life doing discovery and fighting all kinds of expensive legal cases trying to defend yourself because your organization doesn't want to let you go and they want to hold you up there to catch all the arrows and divert them, of course, from somebody else.

So the difficulty is, that as a CISO, we don't always have that type of top cover we should have. And so thinking that if we get a professional association that can essentially like a homeowner's association do a mass buy on. Insurance for CISOs. I'm interested in that. Now, [00:11:00] we know this is a highly debated topic, but we think this is going to help out.

Number 7, CISO Retreats. We're going to predict a change from massive conferences to exclusive retreats that are going to attract the attention of CISOs. For example, Team 8 has a CISO Summit. Merlin Ventures has Safaris. Ira Winkler of Securementum has put together CruiseCon, which I mentioned a little bit earlier.

I'm going to be there. Tom Mess has put together a SCISO, Skiing CISO, Cybersecurity Summit up in Canada, eh? And we think CISOs are often at a point in their lives where they're looking for experiences and adventures. Going to RSA in black hat, kinda like being cattle. You're shuffled around from room to room.

It's not really a five star experience. And although sometimes you get invited out to really nice dinners and of course you go to RSA, it's usually the parties, but we think that companies that shift toward these types of sponsorships are going to have superior interaction with CISOs because not only are they going to be able to have a platform for education and informing, you're creating a collaboration platform where you can do [00:12:00] networking with your peers.

And it's very helpful to have other CISOs and other security professionals in your circle so you can exchange ideas and be aware of what's coming on, potentially even looking for your next job. Number eight, automating expensive cyber tasks. AI has taught us a lot of things that used to be hard. Can now be automated.

Now we don't anticipate you can automate everything in cyber. We do think 2025 will be a huge year for this. For example, you can expect agentic AI to be the next big thing in our industry. If you haven't heard of this, it's basically if this, then that. As Zapier meets generative AI. So here's a lot of models you can plug and play to automate things.

We also expect more cyber functions to use policy as code. One such example, security reviews of network diagrams. There's no reason for a human to do this anymore. Tools like Open Policy Agent make it easy for companies to say, in code, that this is what is allowed for [00:13:00] any Terraform script. And it violates this rule, but your policy says this network diagram should be denied.

Put a link in there for a little bit more if you want to get into that. Number nine, browser based security is on the

rise.

[00:13:14] **G Mark Hardy:** If we look at how most people spend their time at work on the desktop, it's fair to say that most things involve the browser. Of course, you've got email too, but between those two, that's going to attract a lot of your FaceTime and your interaction.

Now, if we think that browser based security solutions are lacking, better ones make a lot of sense. Now, we're not just talking about replacing the Chrome browser with a security themed browser like Island or Talon. That's good stuff. And those are valid products, but we're talking about Chrome browser extensions.

Two such examples are DefenseX and LayerX and they can do things like look at the website you're visiting and perform data loss prevention in Chrome. In addition, they also do things like take your Gmail [00:14:00] attachments that you might want to open and open them in a sandbox tab so that you minimize the potential damage of a malicious phishing email, just in case it has something that says, oops, your files are encrypted.

We think this makes a lot of sense and we anticipate a lot of CISOs are going to explore this as a way to solve AI security governance and lower the threats of phishing. All right, number 10. Post quantum cryptography goes on the main stage. we've heard a little bit about quantum and, so some of those quantum stocks took a huge nosedive recently, when the CEO of Nvidia said, yeah, we're about 10 years out, maybe more from having meaningful quantum computing.

Nonetheless, quantum attacks are getting closer to becoming a reality. When that does happen, you shouldn't get caught unprepared. So we think 2025 is a good year to prioritize post quantum cryptography. Now, you don't have to buy new solutions, you just need to adopt modern ciphers. For example, you can update your TLS ciphers to use post quantum ciphers [00:15:00] like CrystalSkyber, which has been approved by NIST, or FrotoChem, which has been approved by ISO.

Now, don't forget to upgrade your VPNs as well. But what we're talking about then is creating a long tail of post quantum crypto Protection. Why? Because adversaries will record all of your encrypted stuff on the opportunity that when they get the computing power, they can go ahead and replay it and crack crack crack.

Now, we're not talking about necessarily cracking symmetric cyphers. That's not going to happen. You're not going to use quantum to break AES. You're going to go, for example, the key exchange. So whether it's a Diffie Hellman or whatever it's happened to be going on, when you get to the asymmetric cryptography, That's where you go ahead and have the potential vulnerabilities for quantum cryptography.

And so it's a key exchange that'll be compromised. Now granted, five years from now, 99. 99 percent of what you have is probably obsolete. But for 0. 001 percent of the net worth of Satoshi, or Elon, or federal [00:16:00] government, or something like that, yeah, there could be a lot there. So be aware of that. And, Also think about third party risk assessments so they can include that in your tool set as well.

Okay, so those are 10 ideas I'm welcome to hear if you got more Let's go ahead and exchange if you're on the YouTube channel. Let us know if you're on

LinkedIn Give us a little post and say, Hey, here's what we think are going to happen for 2025. And then we'll go back and look at it a year later and see all you do.

Those who get it right, great. You get a teddy bear or something. But the reality is, that things are constantly changing. We know that as cybersecurity professionals, we not only have to be aware of all the current requirements, but we have to be educated and continuously learning to take advantage of the opportunities that are out there.

Think ahead. Windows 10 goes out of support in October of 2025. Bye. Are you fully ready for that? This is a Windows 10 box that I'm recording now and I'm going to probably stretch it out till then, at which [00:17:00] point I'm going to go ahead and just say, yeah, bite the bullet and update because this older machine doesn't have a TPM.

What about for an enterprise level? What's that replacement cost of equipment? Have you gone through and cycled through everything? If you've got a three year replacement cycle, pretty much everything you bought in the last three years has got a TPM in it. All right, full disclosure, this machine will be eight years old.

What if you don't? Or what if you're dealing with embedded systems that are running Windows 10. Or even I've seen Windows XP in medical stuff. Start thinking about that. Make 2025 the year of advanced preparation. Prepare yourself and your career with continuous education. Continue to listen to CISO Tradecraft.

We hope you're part, we are part of your professional development plan. And we offer things such as, say, ISACA.

CISOTradecraft. com will allow you to go ahead and get CPEs for some of the learning that we provide. Take advantage of that. And then also look at your enterprise. Look at the direction we're moving. Try [00:18:00] to anticipate things. What you want to be able to do is brief your leadership. on what's coming before they read about it or hear about it.

And if you're viewed as a security leader who understands what the future's about, then you're going to be in a much better position to influence those above you to get the budgets that you need and hold on to your job quite honestly, in the event that things get a little bit rough. Anyway, hopefully you will have a very great week and a great 2025.

Until next time, this is your host, G Mark Hardy. Stay safe out there.