#162 - CISO Predictions for 2024

[00:00:00]

[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 co host, and today we're going to be talking about predictions for 2024. Now, hey, if you enjoy listening or watching CISO Tradecraft, I'm sure you love earning CPEs.

We've got certs. Of course we need them. So we've teamed up with the ISACA Central Maryland chapter to bring you live online their 20th annual day with G Mark on Wednesday, the 10th of January, 2024 starts at eight in the morning, ends at four in the afternoon, Eastern time. And you'll earn seven CPEs, which are good for ISACA certs, ISC squared certs, even SAN certs, and pretty much any other.

Cert issuer that's out there. What a great way to start out your new year. So check [00:01:00] out the link at CISOTradecraft.com/ISACA, I S A C A for more information and to register. Now there's a limited number of seats, so don't wait. Anyway, happy new year. Okay. So 52 episodes ago. Wow, we did our predictions for 2023 and so, well, it's that time of year again.

And so we're going to review our ideas from last year and see which ones we got right, which ones we got wrong, and maybe which ones could have made you a ton of money. A hint, we did not predict NVIDIA going to the moon. now there's a number of pundits that offer predictions for the new year, and you can do a Google search on security predictions for 2024, and you'll get dozens of ideas.

Now we came up with our list without looking at those. But it's worth a browse over a cup of coffee. Now, as you listen to this episode and even look at other predictions, why not try to identify trends that can help you in your career or help you better defend your enterprise? Okay, so [00:02:00] let's get started.

Now, the first five will be from my co host and the last five are mine. Now, some we agree on and some we don't, but I want to share those all with you to present them for your consideration. The first one is this. CISOs are going to flock to buy private liability and DNO insurance, directors and officers.

It also becomes the norm for CISO hiring agreements. Hmm. Well, let's look a little bit of the background on that and I'll tell you whether or not we think this is going to take place. For those of us who remember Joe Sullivan at Uber back in November 2016, there was a breach that exposed about 57 million customers.

The way that all worked out is it appears that they paid a 100, 000 bug bounty to two hackers in exchange for an NDA. Well, what happened was, is that that was going to be kind of, okay, we sweep it under the rug, but a new CEO came in, Dara Khashrashahi, and he found out, fired the CISO, and called the regulators.

[00:02:52] **G Mark Hardy:** So he was ultimately found guilty by a federal jury in May of 2023. Joe, was judged to by [00:03:00] Judge Orrick to have a $50,000 fine and 200 hours of community service. And the judge said, I'm kind of letting you off easy, but this is not gonna be the case in the future. It's a one-off. Okay. And then more recently, Tim Brown, the CISO for Solar Winds, October, 2023, was gone ahead and served, with.

Charges because back in October, 2020, there was a cyber attack, allegedly by our Russian state operators against SolarWinds. And the claim is that Brown made money, by selling stock before disclosures misrepresented the state of security, et cetera. Now, for those of us who are CISOs or aspiring to be CISOs, this could potentially have a chilling effect.

This hasn't happened before, and now it's starting to occur. you scary thing to get. would be something called a Wells Notice. Now, a Wells Notice, if you've heard of it, but you're not sure exactly what it is, it's a letter sent by a securities regulator to a prospective respondent, notifying that person of the substance of charges that the regulator intends to [00:04:00] bring against them, and affording that person with the opportunity to submit a written statement, ultimately to the decision maker.

Now, The etymology behind that, where does the term Wells notice come from? Back in 1972, the SEC chairman back then was William Casey, and he appointed a committee that was chaired by John Wells and therefore was referred to as the Wells Committee to review and evaluate the commission's enforcement policies and practices.

And one of them that came out of it was this particular document. Now, let's think about it for a minute. Do you have private liability and director and officer insurance? If not, then will your company pay for it or will your organization

pay for it? And if neither of you are going to pay for it, do you think it's wise to continue without that type of protection?

Now, what we're going to see is an evolution of insurance and maybe a lot of efforts to try to figure out how to price this. And I'm not sure how insurance companies are going to effectively adjudicate their potential risk for a CISO, because a lot of these issues come [00:05:00] up. from a liability perspective, literally years after the alleged event took place.

So that'll be an interesting one, but I do think that we'll see more interest in insurance. And maybe if you're a CISO and you're looking for a job change or looking for your annual review, putting that in your package probably makes a lot of sense. Okay. Number two, the CISO reporting structure changes.

No more reporting to the CIO. Okay. Well, that's something that I'm not so sure the CISOs are being sued. They're having a bigger presence in SEC reporting, and therefore they're going to want to separate them out and things like that. No, I'm not sure I agree with this particular prediction. Why?

There's a lot of different ways that CISOs can report, and I might not have them all, but a lot of them include things like reporting directly to the CEO and Or to the CIO, which is the most common statistically, the Chief Financial Officer, Chief Risk Officer, Chief Technology Officer, and even the Chief Operating Officer.

Let's walk through a little [00:06:00] bit of each one of those, because if you're familiar with what your organization has as a reporting structure. Or, if there is no CISO and you're creating one, to whom will that person report? The advantage of a CEO is, well, of course, you're front and center, and you've got the big boss's attention.

The disadvantage, and now these are opinions, is that the CEO is really busy. A CEO should be outwardly focused most of the time. They're out there dealing with investors, they're dealing with big customers, they're dealing with regulators, they're dealing with the government, they're dealing with potential opportunities and things like that, and they're not going to give you the time of day necessarily unless it's a big deal.

And if security is a big deal all the time that requires a CEO's attention, there's a problem. And so you might want to think about that one. The CIO, which has been traditionally the way we've done it, is we thought of CISO being reporting

there as part of the information or the IT function. Now there's a built in conflict of interest there.

If the CIO is given a mandate by management to say, make sure this thing is up and running by the 31st of [00:07:00] December, or on the 1st of January, we're going to be talking to a new CIO. Do you understand? Then the CIO is under pressure to get something out the door. The CISO might say, Hey boss, hey boss, there's security missing.

There's, there's a shortcut here. This is not right. And the CIO is going to say, shh, quiet, my job's on the line. If you make any noise, your job's on the line. So there's a potential conflict there. In addition, we've often thought from a budgeting perspective, as IT security budgets as being a percentage of the IT budget.

Well. Some people argue that that's a reasonable measure. Some people say you might as well measure it against the coffee budget. They're not as, as correlated. I think what we're seeing though, is IT security becoming more pervasive into terms of things such as, well, concern about liability that we're talking about.

Looking at security awareness training, which is going to be more of an HR type of a function, dealing of course with the networking and getting things up there in the cloud. We might find out that cybersecurity doesn't [00:08:00] neatly fit into the IT world. Certainly reporting the Chief Financial Officer is nice when your boss can get you the money you need.

Anybody who's ever had to go through budgetary review and try to compete for funds against all the other departments. If your boss likes you and they understand what you're doing, you could probably get your funding a little bit better. The hard part is always you're isolated from the business units and you're not actually kind of touching or operating with what everybody else is doing.

So there's a little bit of an ivory tower problem there. If you report to the Chief Risk Officer, Chief Risk Officers typically report up to the board, and that's great, you've got kind of a conduit, but I think we're seeing more and more that CISOs are getting a chance to talk to their boards, if not on a regular basis when they just simply say all is fine.

Things are going well. Thank you for letting us talk to you. We'll talk to you again in six months. you get called up there when something goes on. I've had the privilege of briefing the board when there is a breach. In fact, one [00:09:00]

organization I got hired on as a CISO and they said, Oh, by the way, you get to talk to the board next month.

it turned out that the concern there of, wow, it's going to be a scary event. Wasn't so bad. Why? Because in briefing the board, it's pretty much a matter of laying out what happened at executive level. Don't get in the bits and bytes. But we talk about that in some of our other episodes about briefing the board.

Here's the business issue. Here's the problem we had. Here's what we did to fix it. And here's why we think it's not a current problem. And here's why there's no downstream liability. If I'm a board member and I hear that, it's like, okay, fine, let's move on. Now the chief risk officer, again, potentially being compartmented into that reporting up to the board isn't as associated with other business units.

So it's a great way to have that conduit but I think you might also get that conduit on your own as a CISO if not on a regular basis, however. The chief technology officer, if you're a company that's building IT tools and things like that, is a great place in terms of making sure that your product has security built in.

However, a lot of what we do as a [00:10:00] CISO is the operational element of the corporation or the business itself. And so you might build great security into the widget. The company that's operating, that's employing the people that runs the factory that is building the widgets may be woefully unsecured and you don't have the points of contact there.

And the last one I mentioned was the Chief Operating Officer. Now that's a relationship that I've had before that I think works. Why? Because if a CEO is outwardly facing, then a COO is inwardly facing. The Chief Operating Officer is aware of what's going on in the organization. He or she is going to be a busy person, but talking to you would be a normal part of that routine.

This is a relationship. This is something where even if you're not having to brief them on a security vendor status on a regular basis, stay in touch. A lot of what we find out is that at the level of a C anything, in this particular case CISO, and if you notice every other job we talked about in this little section is a C level person, is at the political layer.

Beyond technical competency, [00:11:00] beyond management, beyond leadership. And quite honestly, it's just the nature of how things are. Not politics from the sense of elected politics, but understanding sources of power,

understanding how to negotiate effectively to give people what they want without giving up too much of your own by avoiding those who have power, who could respond negatively and damage you if you're not careful.

All that organizational awareness becomes important. So I'm kind of curious what your reporting relationship is. We'll probably put a little survey out here on our LinkedIn, just to find out on our own little informal survey, because we've got well over 10, 000 followers on LinkedIn for CISO Tradecraft to, instead of relying on somebody else's survey.

We'll find out. So let us know. Okay. Number three, more CISOs will get implicated in lawsuits, but the lawsuits rule in favor of the CISO. Essentially, the CISO did good enough for cyber to be good. well, I don't know that as I mentioned, that was my, my co host, but. Be careful what you wish for. [00:12:00] Now, we think about, well, who's next, right?

I mean, we've heard a couple shoes drop in 2023. Richard Bretto, he's at Progress Software. For those of you who've heard of MoveIt, the transfer, there was a compromise back in May of 2023 by the Klopp group. is that person next? They're not wishing anything on anybody. the concern is about the lawsuits is, is even if you're vindicated, you lose.

Think of the time, the money. the emotional trauma potentially that inflicts upon you in terms of your family and also just in terms of professional reputation. And so as a result, although there may be an opportunity for more CISOs implicated in lawsuits, let's think a little bit about some of these SEC rulings that came out.

And the SEC ruling which kicked in finally in December of 2023 with respect to things like putting out 10ks and announcing whether it's a cybersecurity event. We're starting to see a lot more of those. What that suggests then is that if boards and organizational [00:13:00] management understand that their bias needs to be less toward protecting or hiding information and more toward disclosing information, I think there may be less basis for us to go ahead and have to worry about.

Coming after the CISOs, for example, because common business practice is going to be to fess up early so that that information is made available. Again, a lot of the times the regulators care about material information, material being what would an average investor consider to have affected his or her decision, whether or not they want to invest or stay invested in a company.

Number four is it's harder to find cyber talent since universities are not graduating as many students and this plus inflation Increases will result in a major spike in cyber salaries. Well for those of us to receive cyber salaries We could only hope so for those who pay them We're kind of like, gee whiz, it doesn't sound good, but let's take a look at what's out there.

[00:14:00] Based on my research on the cybersecurityguide. org, I found out that they list at least 178 different bachelors of cybersecurity degree programs in the United States of America. That's a lot of them, and the prices are all over the map. Florida Polytechnic University was estimated at about 12, 000 if you're in state, Rochester Institute of Technology, over a quarter million dollars to be able to do that and everything in between.

Now, I don't have any insight or comment in terms of the quality of these programs. I know that when you get a degree from certain institutions, it does carry a cachet to say, Oh, well, I graduated from this or something like that. But the reality is what you're looking for is a skill set. Now, I've taught at the master's level as adjunct faculty.

And one of the things you find out as an adjunct faculty is that you're not, of course, full time, you're not quite second class, but sort of, kind of in the faculty world, but you're a practitioner. This is stuff you do on a daily basis. You come in, you said, Hey, I'm going to come out of the cold. [00:15:00] I'm going to teach a class or two.

Well, the advantage of that over a professor. Someone who's been in academia for years, and this is not a criticism, it's an observation, is you're, well, a practitioner. If you observe things, if you read about things, if you comment about things, that doesn't necessarily make you a practicing, practicing expert.

I can read an awful lot. about flying a 737. But does that make me a better pilot than someone who actually has stick time? And the answer is probably not. And so consider that the time that it often takes in the university world to update a curriculum, to go through the whole process of changing things, can be a very long time and if you have a math class or a biology class or a chemistry class, things haven't changed a whole lot in the last 100 years or so and so as a result you don't have to make a lot of changes.

But if those who remember G Mark's law, half of what you know about cyber [00:16:00] security will be obsolete in 18 months, you go maybe I need to go ahead and update this curriculum more frequently. And so what we find then is that gap has been filled By cybersecurity certification organizations. And there's

both management certs, technical certs, intro certs, a whole range of things like that.

And having been a teacher at SANS for almost a decade, I'll have to tell you that we were able to update our material quite frequently. In fact, we're kind of required to do so. And so there's a very, very high standard of academic excellence. being held in organizations, even if they're not a traditional edu.

So I'm going to suggest that it's not necessarily going to be harder to find cyber talent. It's going to, might be harder to find degreed cyber talent, but then again, it's up to the hiring manager, as well as the peer group, who's doing the technical review to say, does this person have the chops to do the job, whether or not they get the sheepskin to go ahead and point behind and said, look, I went to a school or university.

Well, we'll see where that goes. [00:17:00] Number five, the cyber industry minimizes external consulting costs to weather reduced revenues during a recession. Okay, well, first of all, we have to see if Jerome Powell pulls off the soft landing or not. The stock market certainly thinks he's going to. If you've had money in the Magnificent Seven, you've had a spectacular year in the stock market, which of course makes you wonder.

You always look at like what goes ridiculously high in one year, statistically doesn't do the same the next year. And also that same group was down about 40 percent in 2022. So be careful, you got a real high beta there. But if you're thinking of throwing all your money into the Microsoft and the Apple and Amazon and all those things like that, be very cautious about that, what you do with your personal investment money, because it has been great, but usually past performance is no guarantee of future, as we've heard that before.

Well, we're not talking about financials. We're talking about consulting costs. And so is there going to be a recession? Let's see, it's an election year with an incumbent. And so as a [00:18:00] result, governments push all kinds of buttons and pull all kinds of levers to try to keep the economy happy so that people will vote for whomever's in office right now.

And so of course there's others, people who are not in office, who are out of power, who are going to do everything to make it look miserable. But the momentum I think is in the positive direction. That said, I have worked with clients who have seen a lower revenue overall. Not necessarily because the economy hit a recession, but maybe their customer base is kind of holding back just in case.

And what I think you're going to see is I agree with this. External consulting costs are going to be a little bit more constrained. We're going to try to do it in house. Should we bring in somebody from the outside or can we figure it out? on our own. Figuring out on your own in the past might have been something that was beyond the scope of people being able to do.

But if you, for example, need to update all your policies, you get your policies to be compliant with the PCI DSS, if you ever tried writing a policy with some of the generative AI, which is going to go in the second half of our [00:19:00] predictions, find out that some of them Pretty good. And to the point where I've done some career counseling with a professional and her expertise is in developing policies.

And we went through a little bit and my career advice was you need to kind of come up with a new line of business because a lot of what you're doing right now is going to be supplanted by AI enabled capabilities where people are going to be able to, if you will, roll their own and get to the 90 95 percent level rather than bring in an expert who has done a lot of policies, looked at a lot of organizations and things such as that.

Again, a prediction here, but I think what we're going to see is less of that external consulting. Okay, how about the, the five that I was thinking of? number six, of course, my first one is AI generated fraud will increase significantly. Okay, well, no, no surprise there. We're starting to see little just snippets of that right now.

But if those of you who remember from episode 141, when we had the Chertoff group on board, we had three categories [00:20:00] of risk that our presenters defined. The use of an AI as an instrumentality of a bad actor targeting AI systems themselves and the unintended consequences of AI. such as uploading proprietary information, thinking that, hey, it's going to write me something better.

And all of a sudden it's just been coughed up. Well, the thing with AI generated fraud is that it's not the AI that's bad. It's kind of like the same argument about weapons or anything else like that. It's usually it's in the eye of the beholder. It's a person who's wielding that particular tool that could cause it to be used for good or for evil.

Well, AI offers some great opportunities if you can collect information on an individual. And then be able to present an AI generated avatar. If you've taken a look at channel1. ai, which is a new news station where basically all the news

actors are AI generated bots, but they look pretty good and they look pretty human.

Now I haven't seen it in production, but I've seen the [00:21:00] demo. But the danger is some people are told, well, we get trained on certain elements of language. You only need to hear a handful of words or a few phrases and you could reproduce somebody's voice. I had a client recently who called up and said, Hey, I got this weird call, someone pretending to be from a bank.

And they said, is your name so and so? Well, yes. did you do it? You know, very careful that you answer this question correctly. Did you do a 3 a. m. transaction and buy something at Amazon for 2, 000 bucks? Well, no. And things like that. And then afterwards it's like, I'm not going to answer any more questions that are on this person hung up.

Well, what do they get? And I said, well, they got a clear yes and a clear no. And I know that some financial organizations are going with a voice recognition. And so I'm concerned about that. In fact, I try not to enroll in those programs for anybody who says like, yeah, are you good with these things? I'm not good with these things.

I don't want to have to worry about, is my voice being borrowed or stolen or things such as that. And so as a [00:22:00] result, if you have a chance to opt out of those things, you probably should opt out. But I think we're going to see more AI fraud taking place that way. Because the concern of course is both input and output.

People putting stuff in there and then bad things coming out as well. Number 7. Shadow AI will result in hidden vulnerabilities. What do I mean by shadow AI? We've heard of shadow IT, right? People going ahead and provisioning systems and not going ahead and going through IT. Well, guess what? We've got shadow AI right now.

There are people who are going to go ahead and they're going to try to outsource some part or all of their jobs to an AI. Large language model, hoping that they can A, improve their quality of life or improve their performance or a little bit of both. The danger in my opinion is this, is that the people who are doing this are not necessarily gonna understand what the.

Risks are, but they'll understand what the potential benefits are. So sensitive information going up, [00:23:00] coming back and relying upon, if you will, the sort of equivalent of a crowdsource recommendations. And I had even seen

situations where somebody having used, in my opinion, very obviously, a, an AI model to generate a whole bunch of paragraphs.

went up to a executive who was thinking about AI strategy and said, Oh, I need to rethink the corporate strategy based upon this input. That's really good. And he's like, no, that was AI input from somebody else who was just, you got to figure this out. So do you have a policy on AI? Do you have a policy of who can use it?

And what are the consequences if you're. Using it, and you have not previously disclosed the fact that you're using AI for a particular business function. That's the solution I think you need to take. Because if you're not doing that, then people are going to try it and they're going to work it out. And in some cases, they get some really good results.

But it's that margin, it's that one or two or three percent where [00:24:00] big problems occur that we have to be careful of. And so that's what I'm suggesting as you look at, carefully is the fact that your people have figured out AI. ChatGPT had what a million users within the first four days or something like that and a hundred million users in the first year.

It's Organizations over 1. 1 million have the API SDK to be able to work with it. It's here It's not going anywhere. And as a result, we got to be very very careful about it Which kind of reads me into number eight, which is the large language models The LLM attacks will become a new vector for AI enabled companies Now, what do I mean by that?

Your only, your model is only as good as the data it trains on. And so we have things like OpenAI's GPT 3, and of course you can get ChatGPT 4 if you want to pay for it and other things like that. But what's happening is that we found out that it's not so much garbage in, garbage out. If you train [00:25:00] on bad data, garbage in, garbage stays.

And then it gets pregnant and gives birth to triplets, as Nito Kubain had said once. And it's kind of, it's going to continue to give you the bad stuff. And so there are a couple ideas. One is which is going back toward the attack and saying, can we poison data models with information and it's deliberately wrong so that this output is deliberately wrong and hopefully an adversary or a competitor will use that.

Or conversely, are there ways to create proprietary models such that the bigger model system doesn't learn and doesn't train with what you're doing? So one of

the concerns that we had from bad actors working with generative AI is that if they put in, you know, how do I hack this? How do I break this? How do I damage this?

How do I destroy that? Those are being fed back into the model, learning to say, Hmm, maybe we should block that or maybe we should obfuscate that information. [00:26:00] But it takes something like Chinchilla, which is an LLM. developed last year by Google DeepMind, it 3, even though it's a quarter of the size.

It was trained on about four times the amount of data. And so what we're finding then is these offline models may outperform the online models and they allow for prioritization. So while we hear about these voracious models trying to ingest all information and some lawsuits being filed saying you're going after my copyrighted data, my songs, my books, my movies, my newspapers, my articles, etc.

The alternative may be is that somebody's going to say, you know, I'm not making this available to you. We're going to keep all this stuff behind an inaccessible paywall or more restrictive, and it's only going to be available in this closed LLM. So it will be interesting to see where that goes, but for those who are using open LLMs, I think you're going to see more attacks and then [00:27:00] organizations making a blunder or some strategic error based upon what they thought was correct.

And that goes beyond that lawyer who ended up getting sanctioned along with his law firm by essentially using ChatGPT to quote cases that never existed. And he doubled down on that. So you can Google that and look that up. That's a little bit out of the scope for this particular talk. Number nine, cyber insurance exclusions will tend to normalize and will prescribe and proscribe activities that must be done if payout is to occur.

Okay. So this is something that I've noticed. I do carry professional liability and general liability insurance. I've been doing that for a lot of years. I like to consider myself a cash cow, for the insurance company, cause I don't want to deal with claims and things such as that. Plus, I've been doing this for a while, so I try, try to be very good at what I do.

But, I did receive something that, from my insurance company. It says, quote, new endorsement. In light of the continually [00:28:00] evolving cyber risk environment, beginning in 2021, all Hiscox USA policies will include specific

language affirmatively stating whether we are covering or excluding losses caused by cyber events.

If you renew your coverage with us, Endorsement, exclusion, privacy and cyber incidents will be added to your policy. This endorsement potentially reduces the scope of coverage under your policy. End of quote. So they're backing out of this, just like Florida companies saying, we're not going to cover you for sinkholes, but you know what, the coverage just goes down, but the premium went up.

In any case, that's one of those things where I think the de facto standard policy is going to start to exclude that. Now you can buy these writers. And you can add them to your policy. But what I think has been interesting is the evolution of cybersecurity. 20 some odd years ago, wow, it was like late 1990s.

Mark Fabbro and I, we were trying to go ahead and convince [00:29:00] insurance companies that if they had a standard assessment of their target organizations, they could lower the risk. We would come in there, we would review the security. The client would pay for it. And in return for being able to validate that they were a lower risk, the insurance company could charge a lower premium because they expected less loss.

the premium reduction would be greater than the cost for our particular engagement and everybody would be happy. They looked at it as like we had a third eye and 25 years later, of course, that's what's happening. And we're seeing that. So again, as I say, if you're three steps ahead, you're a heretic.

It helps to just be one step ahead. In any case, what I think you're going to find though, is that as we look at the potential increased liability for CISOs and other security executives, that insurance companies are going to standardize. It's not going to be this company covers you on Thursdays, this company covers you on Wednesdays, this one does it on weekends, but rather they're all going to have similar coverage.

It's been normalized. And so I think we're going to start [00:30:00] to see less variation across the companies and more of it core element of things. Now, why are there exclusions in insurance? Policies. Quite honestly, because insurance companies are in the business of cashing checks, not writing checks. And so what you want to look at is things that you cannot easily mathematically model or that indicate they might be chaotic.

So, for example, a life insurance policy will cover you if you get hit by a car, for example, or you get some horrible disease and die of it. But they're not going to cover you in the event of nuclear war, insurrection, or zombie apocalypse. Why? Because that could take out thousands or tens of thousands of people all at once.

And as a result, that's hard to insure against. Now, companies that had business interruption insurance four years ago, that did not have an exclusion in their policy for pandemic, they would go ahead and say, hey, pandemic, we need to get paid. I don't know, I don't have business interruption insurance. In fact, my opinion is business interruption insurance only provides for the orderly demise of your company [00:31:00] because you can pay your bills while you're out of business and your customers go someplace else.

But in any case, I'm pretty sure every policy today has that exclusion and it's not because they're mean or they're jerks or whatever. They just have to recognize from a risk adjusted perspective that you can't insure against. Everybody having a claim all at once. And so as a result, what you're going to see then is things that make sense across the board.

I've also reviewed a, or reviewed a cybersecurity policy recently for an organization that I work with. And I thought it was quite comprehensive. The exclusions were, in my opinion, believe it or not, reasonable. And so this common business practice that they were doing, if you drove right down the middle and you didn't do something stupid on the left or stupid on the right.

You recovered and lurked pretty well. last one that I had, which was, I can't really justify it, but I'm thinking self driving cars will encounter regulatory setback if you're on San Francisco or other parts of the world. I think I saw some in Phoenix when I was out there. you see these cars walking around with all these sensors on the top and [00:32:00] little blinky lights or whatever, and there's nobody in the front seat.

And so you've got these self driving cars. They're not moving very quickly and they tend to stay in urban areas and a very concentrated place. And there have been a couple. Accidents. And I think both cases where they were reported, it wasn't the car's fault, so to say, it wasn't the software error and things like that, but being in cybersecurity as long as I have and knowing what the capabilities and limitations are of systems makes me a little bit of an eludite, meaning what?

I'm a little bit hesitant to embrace some of these technologies where It has a capability to be a life or death type of a situation. As a pilot, I don't like

autopilot. I would rather fly the plane myself. I'm going to land, I'm going to land it myself. Now, if it's zero, zero, okay, fine, but I'm not instrument rated.

So that's not an issue for me. But in some particular cases, we find out that, these vehicles are getting more and more sophisticated and that's great. But the problem [00:33:00] is boundary conditions, and the boundary conditions are things that the programmers just didn't think of, whether we go back to a Tesla a couple years ago where a flatbed truck pulled across, there's nothing on the flatbed, so all you saw was a horizontal line, apparently didn't register as a threat, and boom, drove right underneath it and turned the car into a target top.

Unfortunately, the driver was killed in the process. Is that a fault? of the company. I don't know. Lawyers want to think so because anytime you can go ahead and and sue you, you'll do so. But I think their organizations are moving forward. it may get to the point where we're going to have to sequester self driving vehicles from non self driving vehicles.

We have our own little, you know, special lane, so to speak. And for people like me who like to drive old cars, you know, I still have my first car. It's over 60 years old. not that I bought it new, but the point is, is that I like old cars. And, yet I may end up being a situation where, no, you can't get in the same lane with all these self driving things because you're a human and [00:34:00] you're chaotic.

So, we'll see where that goes. Okay, so real quickly, let's see how we did last year. So, episode 110, we had about proactive identity management was the first one. Automating. Our provisioning of access minimizing the digital blast radius. I'll give us a partial success on that one because zero trust is helping to minimize the blast radius, but also because it's not an overnight thing.

It might be a three year journey to get there. So we'll take a half a point maybe. Number two, convergence of security tools. We talk about things like Microsoft or Palo Alto or CrowdStrike or Cisco, companies that have a lot of capabilities, either buying other companies or advancing their scope of what they have.

We're seeing this happen, but there's more tool categories emerging. and so some tools are going to grow or the capability is going to grow faster than vendors can consolidate. So there's some vendor consolidation going on, but I don't see the convergence of security tolls per se. [00:35:00] maybe I'm wrong, but I'm going to score us a zero out of one on that one.

collaboration technology. We're going to be focusing more and more and Zoom's going to take over. And I think we missed that because the return to the office with the hybrid working three days a week, is, seems to be kind of the corporate norm, plus or minus. And so I think the effort, effort on collaboration technology has been replaced by the good old fashioned collaboration technology face to face.

Number four, evolution of the endpoint. Getting more and more like Chromebook or browser isolation? not necessarily. I mean, there's vendors like Island, that have their browser and that looks pretty good. And so there are other, companies out there that do things that will do, sandbox browsers, authenticate, for example.

But I haven't seen that really taking off. These companies are not becoming unicorns and so I would say now we miss that one. number five. Chatbots, increase of bots. Okay, yeah, we got that in spades with [00:36:00] ChatGPT. Didn't quite define as ChatGPT, but yeah, we'll take full credit for that one because we thought there'd be more use of bots and chatbots and then ChatGPT has just kind of done that in steroids.

Number six, we thought there might be vague and unclear cyber laws in 2023. I think the SEC has cleared things up quite a bit. And so what we find out is that, to a certain extent, they've made a lot of clarity out there. some people argue, what is materiality? It's interpretive. It's, you'll know it when you see it.

But materiality, as we said before, is something that would affect an investor's decision whether or not to stay invested or to invest in a company. And materiality is going to be independent. If I lost 50 cents out of my pocket. That's not a material loss. If I lost 50, 000, that's material to me. Now, if you're Elon Musk and you lost 50, 000, it's probably not material.

You lost 50 billion. Yeah. And so [00:37:00] what we find then is materiality is specific to an organization. And so I think that there is some vaguery out there in terms of, there's no law that says you have to patch within X days, that leaves things up for interpretation. And that's probably okay in my opinion, cause we haven't figured it out yet.

It's like the story of the university chancellor when they put in a whole new common ground. I'll plant a grass everywhere. They said, where do you want to put the. the cement trails. He says don't put any in for the first year. What do you mean? Just let the students walk across the grass. When you see where all

the trails are, next year that's where you go ahead and you put the pathways because people have figured out where they want to go.

So I think that's kind of the way we're going. But things like the SEC requirement report in four days, that's pretty darn clear. Number seven, CISO liability increases. We saw two CISOs being sued. You know, both with, Uber and SolarWinds. So yeah, that's definitely taken place a little bit more so than we thought.

[00:38:00] Unfortunately. number eight, Umbrella IT General Controls Mapping. the Secure Controls Framework didn't really see that taking off. So that's kind of a miss on that one. number nine was interesting. The companies would be less, less truthful during third party questionnaires. Now. In my opinion, sometimes these third party questionnaires are a form of harassment for the CISO.

I get someone said, Hey G Mark, we need this thing filled out by Friday if we can get this deal. And it's 287 questions. And it's a slightly different 287 questions than the last month one that came from somebody else. And so until there is a standard scoring out there, I know there's some companies out there that are working on that.

it's difficult, to be able to have to do that because you have to keep answering these things. Plus, some of these questions are vague and unclear. Like, do you do vulnerability management? Well, yes, of course we do. But in a future breach, they might say, well, you didn't patch fast enough. that questionnaire didn't ask, how long does it take to patch?

It just said, do you do vulnerability management? If you said, what [00:39:00] percentage of your mission critical systems do you patch within 90 days over the last, Six months. That's much more specific, but that's maybe too specific for one of these generic questionnaires. So there's just so much risk assessment you can do with these things.

The other thing also is that your SOC 2 might be being filled out by computers that might have wrong input. So companies like Drata and Vanta are being able to go ahead and populate some of these long reports. Are the auditors just rubber stamping them saying, well the computer wrote it. It must be right.

Or do you actually go ahead and pull to ground truth and try to figure that out? We'll see where that goes. And the last one that we had was cyber defense will become more difficult because of people. Now, security awareness companies

like know before wouldn't love you to believe that's true because you need to go more security awareness training and I get that.

But are people becoming less of a critical path for security activities is maybe the better question to ask. If we're being able to automate things or get them to the point where they're not so critical [00:40:00] anymore. That is to say no humans in the loop, then they're not going to be a potential source of vulnerability.

social engineering has been an issue and it's always been an issue. But, for example, we've seen a change in social engineering. Instead of just going ahead and calling up and trying to be somebody, call up a help desk in a casino and then try to get credentials reset so they can log in with real creds that can cause some damage.

We heard about what happened in Las Vegas this past year. And other things that we're seeing is that some of the people stuff is saying, Hey. These ransomware actors are going to say, Hey, we'll report you the SEC if that you didn't disclose in a timely manner, just pay our ransom because our ransom is cheaper than the fine that you would take.

But I think that the move toward greater disclosure, the fact that everybody's going to do it now, the fact that you're going to see a lot more 10 K's coming out takes away a little bit of the stigma. And it might take a little bit of the ammunition out of that type of a ransomware attack to saying, Hey, just keep it quiet and pay a ransom and we won't tell anybody.

so that may be diffused as [00:41:00] well. Okay, so it's a whole lot of stuff. It's a whole lot of ideas. I hope I got you thinking about some things that you might be able to think about. Specifically, actionable items. Look at your insurance. Look at your liability coverage. Look at your organization, whether they got your back or not.

And your professional, as well as general, liability should be something that you carry. Just because we seem to be in a litigious environment, and it's not going to get necessarily any better anytime soon. Okay. So for 2024, as I said before, we're going to kick off on the 10th of January. Please go ahead and take a look at cisotradecraft.com/isaca, I S A C A, sign up. You get to go ahead and get some CPEs. You listen to me and see me, of course, it's going to be a virtual environment, but I've worked with ISACA, the Central Maryland Chapter, literally for 20 years doing a day with G Mark. And it's been a real privilege to do so.

And they've allowed me to extend that invitation. To all of our CISO Tradecraft listeners and viewers. So you're [00:42:00] welcome to be a part of that. until the next time, if you are following us on YouTube, or I guess, subscribing, that's what you do on YouTube. Please do so. It actually, it's been very slow getting our numbers up, surprisingly enough.

We can't get rid of the Ads that we don't want until we get to a certain threshold. So, you know, do us a new year's favor and just go ahead and subscribe on YouTube, even if you're not watching all the time, pass along on the other podcast channels, let them know that you're listening to CISO Tradecraft and share with your professional.

Peers, where you're getting your knowledge and your insight, because we think we can reach a lot more people this year and help them out with their careers as well as defend our enterprises. So best wishes for the new year. Hope you're doing well. And until next time, this is your host, G Mark Hardy. Stay safe out there.