[00:00:00] 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, and today we're going to talk about predictions for the new year. Happy New Year everyone, so if you're not already following us on LinkedIn, please do so. You'll get a lot more than podcasts. You'll get some great information with our regular postings there as well. Share with others where you get your good stuff so that we can get additional followers. So let's get started.

It's common for people to make goals and predictions at the start of the new year.  So today we're excited to share with you what we think will be our top CISO Tradecraft predictions for 2023. All right, so well, let's get to it.

We think identity and access management is going to be the biggest concern in cybersecurity [00:01:00] for 2023, and therefore we predict there'll be a big opportunity to do something we're calling **Proactive Identity Management**. Now, proactive identity management consists of two concepts that work really nicely together. These two concepts are **Automated Provisioning of Access** and **Digital Blast Radius**. Now, why do I need to apply these two concepts if I'm already focused on zero trust? I mean, after all, zero trust was a big push this past year and will continue to be a big push. Well, first of all, let's start with a clear definition of what zero trust means. Zero trust started on the premise that organizations are already breached. So you needed to limit the digital blast radius. However, network-based perimeters didn't really help you when you already had a malicious actor with malware beaconing out from inside the network.

There needed to be a shift to focus on securing access on a per user, per asset, and resource level. [00:02:00] Essentially trust nothing, verify everything. Now, this means that Zero trust requires adopting multi factor authentication, conditional user access policies, privileged access management, least privilege, and continuous authentication to say nothing about encrypting.

Pretty much everything. Now, it appears to us that Zero Trust is about minimizing user access to the resource at the time access is initially granted. However, Zero Trust may miss a key concern. Our digital accesses shouldn't be static. They need to be dynamic. I mean, think about it this way. If someone were granted access to a resource, but never use those permissions, we might not even be aware of the that those additional permissions were there were that account to be compromised, and then the blast radius would be unnecessarily large by limiting access to exactly where it needs to be. We can tell very quickly

in [00:03:00] the event of a compromise, whether an account goes bad or if a user goes bad, exactly the amount of damage that individual could have done.

Somebody could have done without an account. See, this is where Proactive Identity Management comes into place. Proactive Identity Management is about enabling business users to get access to resources quickly while ensuring access follows the concept of least privilege. Now, to enable this, we start by creating an environment of automated provisioning.

You can think of it like this. A user submits an access request that needs to be approved by just two people. First is going to be the supervisor who confirms the requester has a legitimate business justification to access the resource. The second approver is the owner of the data hosted by the application.

Now, this data owner ensures the access role requested, and provides the least amount of privilege needed to enable the business objective. Now, once a user access request is approved by the [00:04:00] supervisor, and the data owner, the user's identity can be automatically placed into an active directory group that grants immediate access to the resource.

Now, this means that once an access request receives two-person approval, it can be granted in minutes. We should never have to wait for a system administrator to manually log into an application to add a user to a group or a role. See, once you've achieved automated provisioning, which is going to decrease the friction to get access, Then you can also focus on the second step we call, minimizing the digital blast radius.

Now that term comes from kinetic weapons where when something blows up, you want to know how far away is it going to do significant damage. In the same way, we look at a blast radius in our IT systems to say, if something happens, how extensive could that damage be?

Now to do this, we want to adopt Access monitoring tools such as the IAM Access Analyzer from aws. This tool looks at user identities, [00:05:00] says for example, based on log traffic. We see that the following user accounts have accesses they're not using, so IAM Access Analyzer provides recommendations to revoke this access, or minimize the access. Now, this is a really powerful concept that when automated, Can minimize the impact of data breaches.

Consider the consequence of just one accountant in the procurement department being phished. The accountant likely has access to key IT systems containing billing information, shared drives containing contracts, teams folders hosting

purchase orders, and perhaps even credit card numbers from customers or the company procurement cards.

If a bad actor successfully phishes the accountant, that bad actor has access to all that sensitive data. Now, if an organization adopts automated revocation of access, then the digital blast radius of the accountant can be decreased from every file they ever access to only the last 90 days of files they accessed.

And we [00:06:00] think it's a great way to minimize the impact of data breaches, which wise? The first in our 2023 prediction list. Our second prediction is the **convergence of security tools.** Today, there's so many tools that cyber organizations are buying. Just go to any Fortune 500 company, and they'll usually have at least 40 or more security tools.

Let's just take the space of application security. There's static application security testing, SAST, dynamic application security testing DAST, software composition analysis, SCA containers, secret scanning, etc. If you adopt a best of breed approach, That means you also have to have multiple vendors and multiple contracts.

The end result is cyber organizations spend a lot of their time in procurement conversations, trying to get in-house lawyers to accept contract terms and conditions versus doing the real cyber work. And we think that the friction is going to create a demand for cyber departments to minimize. The number of [00:07:00] vendors and tools in 2023.

Here's a clearer example. Today, developer organizations typically buy GitHub or GitLab as a source code repository, and there's a huge business case to buy something like GitLab Ultimate Edition or GitHub Advanced Security. Now, if you did purchase GitLab ultimate edition, then you would also get access to SAST, DAST, container scanning and dependency scanning tools. Note that GitHub Advanced Security is similar, but it lacks a DAST tool. This ultimate addition from GitLab minimizes the need to negotiate SAST tools with microfocus DAST tools, with Acunetix container scanning tools with Anchore dependency scanning tools with Snyk

It creates simplicity for developers to only have to learn one vendor approach and reduces the amount of system administration needed to maintain tools.

The third prediction we make is that of **collaboration** [00:08:00] **technology**. It's going to really take off. The biggest thing we saw from Covid was the rapid shift to working from home.

Some companies allow their employees to work from home three days a week, whereas others begin hiring remote employees with. This is a new business norm. IT organizations need to reimagine the work from home experience to be more fun and collaborative. Now, one way to do this is through adoption of collaboration tools like miro.com or mural.co.

Both of these solutions provide reusable templates, that allow teams that better communicate and work digitally. Consider a template like a Kanban board. It creates a known format that teams can use to communicate the status of work and shows where opportunities exist. These tools offer hundreds of templates that you can use.

For example, you can choose things like agile roadmaps, brainstorms, business canvas templates. Concept maps, decision matrices, flow charts, Gantt charts, Kanban boards, market funnels, risk [00:09:00] matrices, SWOT templates, to-do lists, unified modeling language diagrams, and even wireframes. Now, the big evolution in tools like miro.com and mural is that they allow you to work on these documents together.

So imagine doing a brainstorming exercise where you have 10 people all putting post-it notes on a whiteboard in person. With technology like Miro, you can create digital post-Its that you can arrange on a digital whiteboard. It'll make your team more effective. It'll also create that fun and engaging atmosphere that teams have missed being away from the office.

The next prediction we have is the **evolution of the endpoint**. If we are realistic with ourselves, and we know that some subset of our employee population will continue to click on phishing emails, this means we have to continually secure our endpoints. We see two technical approaches to solving the issue that which will be adopted by most workplaces.

The first is **Chromebooks**. Now Chromebooks come with auto updates, sandboxes, [00:10:00] and data encryption. You can think of a Chromebook as an operating system that only runs Google Chrome, and since you don't need Java or any other desktop software, that saves your help desk team from installing software, from minimizing the amount of vulnerability management activities that your organization needs to perform, all the help desk really needs to do is to keep Chrome Patched, which already auto updates.

And control the chrome extensions that are approved for the organization. By taking this approach, you don't need to buy five different security agents to install in your operating system. You can save a lot of money from security

tooling by just forwarding your web traffic. If you use tools like Zscaler and CrowdStrike Falcon, then you can get a great view of what's happening in your read only desktop environment.

The other approach to protecting the desktop is **Browser Isolation Tools** like Silo by Authentic8 or concealed brows by conceal.io, you can think of these like a modernized Citrix environment. You'll log into them over your [00:11:00] browser. They spin up a quick container for you to use as a desktop. And after your work is done, you destroy the temporary environment you created.

This way, if you get infected with malware, it's a simple matter to just tear it down and restart the container. Now, while it still remains to be seen, which technology will work better. For most organizations, we think that both Chromebooks and Browser isolation technologies minimize the harm of clicking malicious emails and browsing sketchy websites.

Next under 2023 prediction list is **chatbots**. If you look at the success that OpenAI's ChatGPT is having, we think it's clear that being able to answer questions in a conversational way is transformational. There are many new opportunities here. One example is creating a chat bot that developers in your organization can talk to.

Let's say your organization has internal processes for requesting a penetration test or retiring a server and deleting all the DNS entries, that tribal knowledge needs to be documented. So Bobby the intern, can learn how to do things [00:12:00] correctly. Now, when Bobby and all the other interns have a question, you can point them to your chatbot that tackles their questions.

if the chat bot comes up blank, then have a human answer the interns question and put that question and answer into the chatbot so it becomes smarter. The more you do this, the more efficient your team will be in learning and assimilating new skills and techniques. Another good use for a chatbot will be to help customers. We would expect corporate websites to include a custom chatbot that helps customers request new services, access their latest bill or make payments.

We also think there's a really good opportunity to use chatbots like ChatGPT to help write code. For example, you can ask ChatGPT to write a Splunk query that can spot Microsoft Excel documents, which have embedded macros. You can also ask Chat G P T to create a Splunk query that finds log4J in your environment.

These types of queries can improve your SOX ability to [00:13:00] tune your SIEM faster ways than before.

Our next prediction for 2023 is we'll see more cyber laws passed by states and nation states, but these **new cyber laws written by politicians who will remain vague and provide unclear guidance on what's truly required for CISOs.**

For example, we all know we need to do risk assessments is a cyber organization. However, what is the standardized template for everyone to use for risk assessments? Do we use a Center for Internet Securities Risk assessment method? The C I S RAM is guidance. Do we follow NIST Special Pub 800 - 30.

Do we map to the latest mire attack matrix of ransomware techniques? These standards only say what should be in there, but there really isn't a template that all organizations should fill out. Pen tests are even worse. Another example is logging. We also see regulations. Asking companies to store and monitor log events.

However, [00:14:00] there isn't always clear guidance on what kind of logs are needed and for how long they need to be stored. This is where the problem starts, and you don't want to be found non-compliant by regulators. You see if logging is scoped incorrectly. Then IT teams may be directed to capture every network packet in the organization and store that data for five years.

This is impractical and it's cost prohibitive. However, if the scope only requires log data to recreate financial transactions, okay, sounds good. But guess what? We're going to miss logging the cyber attacks against our company and this means we won't understand how the bad actors got in and how we need to evict them from our IT infrastructure.

The point here is that there's a really fine line of what to collect and for how long. Those types of nuances seem really difficult for policymakers to understand when creating cyber policies and regulations as well as well laws. And that brings us to our seventh prediction. Since [00:15:00] cyber laws will be vague and subjective, **CISO liability trends will increase**.

Uber Technologies, former ciso learned that the hard way. Now, let's put ourselves in the seat of an investor who buys stock in large companies. Now, let's say a company has a data breach, single data breach can happen to anybody. It sucks, but it happens. Just look at how many companies had ransomware this past year.

Now, let's say your company has a second data breach in the same year is the CISO negligent? Who can a shareholder hold responsible? What if there's a third breach? You see, it's a tricky line to measure when due care is being established and when a company is negligent. So for anybody thinking about taking a CISO role, we strongly recommend being under the director and officer liability insurance protection of the company d and o.

If you haven't heard of it, look it up. It's an important insurance.

Number eight is that there'll be a focus to adopt **umbrella iT control mappings** to [00:16:00] all the cyber and data privacy requirements. Now, here's the reason. Let's say you're a technology company who sells a solution similar to Salesforce to businesses within the United States.

You're in scope for PCI if you take payments, hipaa, if you have customer health information, FedRAMP, if you have a cloud solution being sold to the government, CMMC, if you're going to be doing work with DoD and many others. Now, as a ciso, you don't want to go to software application teams and say, complete this assessment, which is only good for one standard.

And when you're done, I'll come back with the next assessment. Ideally, you need an umbrella list of IT general controls that map to all the applicable standards. Then you require each software application team to show evidence and provide attestations that they follow the umbrella list of IT general controls.

Since you meet all your potential customer control requirements. Now your teams can sell software to more clients, which adds new revenue to the [00:17:00] company. If you're looking for ways to create an umbrella list of IT general controls. And consider looking into the Secure Controls Framework, the Unified Compliance Framework, the Profile from Cyber Risk Institute or Audit Scripts.

Each of these umbrella frameworks has already done the work for you, and you don't want to argue with auditors on why you aren't using an industry standard. Additionally, it's a standards change. You could obtain newer versions of umbrella control mappings without having to personally monitor 200 or more cyber and data privacy laws being passed around the globe.

Our ninth prediction is that **companies will be, eh, less truthful in their responses to third party risk questionnaires**. Companies planning to purchase a solution that'll hold sensitive information outside the company will usually perform a third party risk assessment, and typically they send out a detailed

questionnaire of 200 or more questions of software vendors or service vendors, cuz I've had to fill out a number of these things.[00:18:00]

These ask the seller if you have things in place like mfa, security policies and vulnerability management. But the problem is the seller has an incentive to stretch the truth or, well, let's say even lie on these assessments to create new business revenues. So the seller says, yes, we have MFA. But they don't tell you that it's still optional for employees to adopt, and it's not really required.

We think this problem will also get worse when GRC software does automated compliance checks. We imagine a future where companies needing to achieve a SOC two type two or an ISO 27001 certification? We're only going to purchase a GRC software to show compliance. The difference here is rather than having a big four accounting company manually review the evidence from the tool, the GRC tool will be certified by an accounting company.

And unfortunately, we think that automated compliance checks by the GRC tools won't be worth much, and therefore the end result will be a [00:19:00] decrease in the quality of SOC two reports and ISO 27001 certifications. If we go that path.

Our 10th and final prediction is that **cyber defense is going to get more difficult because of people**, not so much that your people aren't going to keep up, but that the economic trend toward a recession is causing businesses to lay off thousands of well-qualified staff.

Meta laid off over 11,000 this past year, Amazon 10,000, Uber over almost 7,000 and even Cisco, like over 4,000. As businesses come to grip with a slowing economy, decreasing sales and reduced revenues, security's going to have a difficult time competing for what's left in the budget. In addition, some of these laid off staff may become threat actors themselves increasing our risk profile, particularly if they hold a grudge against the company, they'll let them go.

A global economy expects to see more threat actor candidates looking for easy money with little to no chance of negative [00:20:00] consequences. Your challenge as a security leader is convincing your management that when the organization is struggling for cash flow, that a tolerable hack in good times may otherwise prove to be fatal.

Attackers could care less if you go out of business. You need to keep the defenses running at full power, even if it means IT security becomes a larger percentage of revenue than last year.

Well, we hope you've enjoyed learning and hearing about our 2023 predictions. If you think they're on point or if we're missing anything, please leave us a comment on our LinkedIn post. Let us know. We'd love to hear your feedback.

Now, every year for the last 19 years, I've had the privilege to do a day with G Mark at the ISACA Central Maryland chapter, and this year is going to be no different. If you go to ISACA, isaca-cmc.org, you'll see what I have there. And by the way, if you like listening to this podcast, why not listen to me and watch [00:21:00] slides and get CPEs?

You can get seven CPEs for that. And so again, isaca-cmc.org. But what I do is I come up with my personal predictions for the year. So these are from January of 2020. and I put them up there, and then I come back every year and I try to hold myself accountable and I, in this case, I kind of have an open field to try to think of things.

For example, the first one was, average investors will be able to buy shares in non fungible tokens. A good sign of a market top. I think that's a win. We saw Bitcoin and a lot of other cryptocurrencies dive in 2022. They were riding really high in November, 2021, and it just looked to me like it was getting really frothy.  So, okay, one for one.

Number two, governments will restrict proof of work cryptocurrency (for example, Bitcoin) mining under pressure by environmentalists driving down the hash rate. Well, two for two. State of New York has gone out and passed regulations saying you can't run certain power plants to go ahead and do cryptocurrency mining.  We've seen a shift from Ethereum going from [00:22:00] proof of work to proof of stake, so I'll take a two for two.

Number three, investors will sell high flying tech stocks by March of 2022 to pay capital gain taxes, driving down PEs and the market. Well, we've had the worst technical stock market since 2008 and it may not be just because people are paying their capital gains, but again, it's tough to call a market top, but it looks pretty close here.  So three for three.

Number four, interest rate on the 10 year bond will reach 3.45. That was ridiculous a year ago.  Now, it actually sounds pretty good.

Number five, midterm election results will be widely contested but will not be overturned. Can I say Arizona? But in any case, I think we're doing pretty well.

Number six, Putin attempts to make Ukraine Mykraine, all right, that was spot on. And so what I've been able to do is six for six.

I'm not so sure about the last one: Some, but not all, auto prices return to earth for [00:23:00] 2023 models, creating advantage for companies that master supply chains. Some companies probably have been able to do so better than others.

Again, what we're seeing is a shift from just in time inventory, which is a very efficient way of doing things to, if you will, hedging your bets and spreading your bets. The move from efficiency to resiliency is going to be the new norm to be able to deal with things such as supply chain shortages.

Warfare disruptions and things such as that. And so I think we'll see that. So I don't know, I'll give myself six out of seven, maybe six and a half out of seven, which is actually not bad. And so if you want to hear what my predictions are going to be for 2023 that are not related to the technology stuff, , come on and , tune in on the 11th of January and hopefully you'll find it a very useful show.

Again, https://isaca-cmc.org.

And as always, please remember to leave us a review if you find the podcast helpful, and if you haven't given us a thumbs [00:24:00] up or a five star, if you think we'd earned it, please do so on the podcast platform you're using.  That helps us reach more listeners as well.

This is your host again, G Mark Hardy. We thank you again for listening, and until next time, stay safe out there.