

#172 - Table Top Exercises

[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. I'm your host, G Mark Hardy, and today we are going to go ahead and talk about tabletop exercises, what they are, why they're valuable and how to implement them in your organization.

So stay tuned. I think you'll learn some really helpful things here. Now, if you're not following us already on LinkedIn, please do so. We provide a lot more than just podcasts. Also, we're up on YouTube. You can go ahead and watch as long as listen. Coming up with some ideas from some episodes in the future would be very helpful to view them because I want to try to go Ahead and put some charts and other diagrams We're not doing that today, but that will give you a chance to look at that So if you haven't done so yet, please go [00:01:00] to youtube and subscribe to the CISO Tradecraft channel Okay, so let's talk about tabletop exercises well, why am I bothering doing episode on this because it's an opportunity for you to provide a forum for your staff to improve your security posture. You can test your policies and your procedures in simulated scenarios so that there's no real emergency going on.

You see, a tabletop exercise is an informal training session. You create a hypothetical situation, and then the team members are going to talk through what the responses can be. And they can help you as a CISO map out your incident response plans, maybe take your existing protocols, refine them, Go through different scenarios like ransomware to see if people know what their roles are and what to do and train people on their roles and responsibilities in the event that the hypothetical event becomes a reality.

Another thing also, and this goes back to some of my Navy background, is that Admiral Rickover, the father of [00:02:00] the nuclear Navy, would say, you fight the way you train. And so as a result, the advantage of doing tabletop exercises isn't so much as you accurately predict some horrible event in the future where it goes exactly to plan.

Never happens. No plan survives contact with the enemy. However, what you will find out is that you've already thought about that. You've already gone through a couple of scenarios. And so when the unexpected happens, people

don't, Stop and stare like they're looking at a deer in the headlight. They go, wait a minute.

Yeah, we considered that already. And let's go ahead. And then you begin making some steps and it gets you off of top dead center very quickly, which is incredibly valuable in a crisis because you don't always have time to stop and think and figure stuff out and be like Jean Luc Picard and go conference and figure out when things are happening.

You're going to respond the way that you've trained, and this is how you train your people. And it's relatively quick and inexpensive because it does not require a lot of fancy electronics, special equipment, and things such as that. [00:03:00] It's going to be a lot of people sitting around a conference room.

You'll have a laptop, some displays, maybe some printouts, and things like that. So, let's think about what this would involve. A tabletop exercise, you can abbreviate that as a TTX, sometimes a TTE. Your team is going to explore the roles and responses during a simulated emergency. So you'll create scenarios, but unlike a full scale simulation where you actually have to go do something, this is a little bit less intense.

You're going to be talking about what you're going to do rather than actually get up there and throw a switch or go ahead and everybody hop in the car and they drive out to the backup and recovery site. So they're not as intense. They don't put you in the same mindset you'll have in exactly as a disaster, but it helps a little bit.

But you also have to be careful that it's not simply a check in the box exercise. Okay, something went wrong. What are you going to do? Well, I'm going to go turn on the emergency generator. I'm going to go ahead and call the backup company. I'm going to go ahead and throw this switch. I'm going to go and do that.

Okay, fine. Yeah, we're done. You want to get a little bit more involved in that. So you want people to play [00:04:00] scenarios out in some sort of a context. Now, there's a hierarchy of events and things like that, where you can basically have just at the bottom level. Hey, here's a procedure. Take a look at it.

Initial it. Let me know that you're okay with it. Fine. That's pretty straightforward. You could go ahead and ask a quiz or something like that. Tabletop exercise then goes to a higher level where you're doing things, you're

interacting. Above that, you can have a functional exercise where you might actually play out a scenario in real time.

Or then a full scale exercise where everybody mans up, all the emergency people come in there, and you respond to a simulated crisis. We're not talking about that, we're talking about something that's a little bit more manageable. Now here's an important thing to think about when it comes to, you know, A tabletop exercise.

This is not a contest. It's not a competition. It's not a test. Nobody's sitting there saying, you did very badly on this particular one. It's designed as a collaborative learning environment. And as a result, you want to create it in a no fault situation where somebody makes a mistake. Great. When I do the tabletop exercises, I tell [00:05:00] people, it's okay to be confused.

If there's any time to be confused or make a mistake, it's right now because it doesn't impact reality. But let's figure that out. So when we go through there and you say, I'm going to go left and you go, well, let's take a look at your procedures. What does it say? Oops, let's go right. Okay, we learned something.

Yes. Great. Move along. And so what this is designed to do is reveal potential weaknesses that you might have and also ensure that people understand what your policies, procedures, and protocols are and the best practices and you do them. Okay, great. Well, one of the first why questions that I think you might ask is that, well, are tabletop exercises required for compliance?

Because, as we know, a lot of times you don't get things funded unless they're required. Well, in a way, sort of. For example, you could run a tabletop exercise focused on SOC 2 compliance. And then you can simulate various data breach or failure scenarios and identify gaps in your current rules. And now you could go ahead and say, well, we've got a proactive approach toward compliance rather than checking [00:06:00] the box.

And now I can go through and update my control definitions, my responsibilities, and the documentation. And then I kind of stream, streamline my SOC 2 compliance process. I'll talk a little bit more about that later from one of the references that I found. Now, from a purpose perspective, as they say, they'll expose your weaknesses in showing that people know how to do protocols and best practices.

It may also show off your strengths too, saying, Hey, wow, we're really on top of this. We know what we're doing. Because this is a human exercise. We're not

bringing the servers in and dragging them in and plugging them in and making sure that they're stress tested and the like. These are people that are going to go through different Steps in process, but they are helping you test.

Your plans. For example, if you have a missing step in your incident response plan, or it's just plain wrong, or out of date, or things like that, as people consult the plans and go ahead and go to work, they go like, yeah, okay, that's not there. Okay, let's write that down. We'll fix that. Or somebody says, I just don't understand this.

Great. [00:07:00] Well, it's, this is a good time to figure out when people don't understand things because now we can fix them. And so what we have then is in addition to our technical testing, because we'll actually want to evaluate, do people know what they're doing? This is our chance to see what people are going to do and how they respond.

Now they're great for, Testing plans and policies and procedures. But if you don't have plans and policies and procedures, and you do a tabletop and everybody just makes stuff up and they improvise, it doesn't tell you a lot. It might tell you that somebody is good at making things up and improvising, but what you really want, if you have a situation where you don't have things formally documented, is to turn that into something formal.

You want to go ahead and get some buy in for that. If management doesn't let you change your plans and policies based on the results, then you're kind of wasting your time. It's nice to go through there and say, Hey, this is wrong. This is wrong. This is wrong. Great. We read it all up. We'd like to change this.

I'm sorry. We're not going to change that. Well, well, come on. We just went through the old scenario and it doesn't work right. Well, we're not going to change it. Okay, fine. [00:08:00] So this gives you better ammunition to go ahead and update things. I know some places have a long cycle time for updating policies and procedures and things such as that.

And as a result, you could either lament the fact that it just takes so long. And admire your problem, or you could do something about it and start the clock ticking. Because if they have a long lead time, start today. Get things done. Now, if we understand why we want to do a tabletop exercise, of course the next question is probably, Who's going to be there?

Whom do we invite? Well, it kind of depends on the purpose of the exercise, right? I could go ahead and have a blue team exercise. And they could respond

to some particular breach and see what they do. Or I could use one for a purple team training where the red team goes ahead and creates a scenario that the blue team has to deal with, but we're not actually attacking our own network.

We're putting these things out there. It could also educate constituents across the organization. We can bring in people. from legal, from finance, from [00:09:00] manufacturing, from production, from operations, so they can see what their roles are going to be in the event of some sort of a cyber incident. And a lot of times people will find out that when you have a major cyber incident, it's not just the cyber people who are dealing with it.

It's all hands on deck, a lot of people are going to be affected, and you don't want people standing around or worse, getting in the way when the people who know what they're doing are are trying to get something done. So when's a good time to schedule a tabletop exercise? Because this takes time to research and write and refine it.

why am I doing my tabletop exercise for this episode? Cause I just did one yesterday, and I spent the better part of a month working on the details, the nuances, understanding the organization, looking at their operations, going through best practices, going through the process, the procedures, their emergency response plan, integrating it all in there, And making it so it's one cohesive whole.

So when it runs, it goes really smoothly. What people don't see is that you've [00:10:00] got a lot of prep work to do. And don't be afraid of doing the prep work, because the closer you are to reality, in terms of your reflection of what's out there, the more powerful that this tabletop is going to be in terms of identifying people's knowledge of what they should do, and spotting the things that they can do better.

Now, if you do this on a regular basis, you get what we would call a battle rhythm. You're ready to do it every six months or every year or whatever. Now it becomes part of your life cycle of your security program. People expect it. They know that maybe in March and October, we're going to be doing cybersecurity exercises, tabletop exercises.

Another time to do it is after you do a major change. For example, what if you move from a managed security service provider to an in house SOC? That's a significant change in how you do business. What a great time to go ahead and do a tabletop exercise to make sure you can work with that new construct that the stuff we used to do for a few years is now.

Doesn't work anymore. And then people, if they're just going by reflex, you say, [00:11:00] well, come on, let's go back and look at the pubs. And if the pubs still have that old stuff there, they don't reflect the new stuff, we need to update them and fix them. So you're starting to see that there's more than just an experience.

What comes out of it are the things that you learn from it and allow you to change the real world. Now, tabletop exercises, for the most part, require, well, a tabletop. I, does it require a simulated network? I don't have to take a cyber range and things such as that. I get a conference room, put all the tables, ideally in a U shape, so people could look at each other, put a PowerPoint on a laptop, get a projector up there, make sure that people have handouts.

And do it in a place where most of the participants are probably going to be anyway. You might not get the budget to get people to fly in from all over the country to do a two hour tabletop, but if they're already going to be there for some corporate event, piggyback on top of it. Coordinate. in advance.

Now, once people are there, you own them. [00:12:00] And I got to understand that it's not to conflict with the real world. Phones off, interruptions, none, unless there's an emergency, unless the building is on fire, don't interrupt anybody during the time of the tabletop exercise. Now that's kind of tough to do, particularly if you pull in C level executives, but if you can get the CEO to stand up and she says, I'm turning off my phone, that's That sets a powerful example for everybody else, right?

Now, how are we going to do a tabletop exercise? The format is basically get your participants invited. They understand what their roles are. Well, their roles are going to be what they do in real life. We're doing a little bit of role playing sometimes if you can't get the right people there. So if a chief financial officer can't be there, but you need someone to act CFO, maybe get somebody from that department and say, for the purposes of the exercise, you're making these determinations.

Okay. Participants gather around a table. You as the leader, presumably you're going to be running this, are going to be able to prompt, describe scenarios, and they're going to be based [00:13:00] upon your organization's plans, policies, and emergency procedures. The goal here is to create a comfortable atmosphere.

Have coffee, have donuts, make people feel at home. And then it's a no risk environment. That's the real key. You don't want people being on their guard saying, I don't want to look like an idiot. It's okay to look like an idiot. In fact,

go ahead and do something idiotic just so you can let people know it's okay to be an idiot.

Then that helps. And what you're gonna do is you're gonna set this up. You're gonna determine your objectives. They may be very specific, which is a good idea, or you could have several of them. And then you want to create a scenario that meets that objectives. Really good tabletop exercise will be a developing scenario where you have what we call injects.

And so you'll set a baseline. Here's what's going on. Here's what's happening. And here's the first inject. Something happens. And then, what do you do? What has happened? What are you worried about? Etc. Here's the second, third, fourth, and depending upon how long your exercise goes, you can do a number of them.

The one I did yesterday, I had five injects. That was a [00:14:00] fairly short meeting, but it worked pretty well. And I'll talk a little bit about how long these things should go, but reality is, if you don't set aside enough time, you're going to go over or you're going to lose stuff. Set the scenario in a real world type of a narrative.

Don't say, in the year 2047, your Blade Runner No, we're not going to go there. What we're going to do is it could be set today, tomorrow, a week from now. There's a major thing going on next month. Okay, put it that. But don't put it five years in the future. Nobody knows what it's going to look like then.

You plan your logistics, which means you've got your IT, you've got your cable, your internet connectivity, the HDMI cable. I went through three of them yesterday before I found one that worked. But we did that before everybody showed up. We had food. Food makes people happy. Go ahead and think about that.

Give everybody lunch. And then, don't forget, have a scribe. If you're running the thing, you can't be documenting all the lessons learned. When you say, that's awesome, I love it! Somebody needs to be writing down, this is a good thing. Because otherwise, you go through the [00:15:00] exercise, and what happened? Well, we had good lunch, and we got off the other stuff, and now we've got to play catch up because there's 100 more emails in your inbox.

Not the outcome you want. What you want in an outcome is to have measurable value. So, your tabletops, as I said, They're not tests. They're not competitions. They're designed to be collaborative and what you want to do, and here's the

reason you do them. We want to identify where our shortcomings and weaknesses are when there is not a crisis rather than wait until there is a real crisis where the Consequences are so much worse.

Ultimately, you want to be able to collect lessons learned. If you don't do lessons learned, if you remember your Incident Response Plan, PICERL, Preparation, Identification, Containment, Eradication, Recovery, L, Lessons Learned, they become lessons lost. And like George Santayana said, those who do not remember the past are doomed to repeat it.

So we do not want to repeat our errors, so capture them and make sure we're doing that. You don't have the pressure of a real [00:16:00] emergency. As a result, you can slow things down. And as we used to say in the military, when you're doing an exercise and there's a learning opportunity, stop the clock, stop the problem.

Alright, let's look at this, discuss it, ready to go. Alright, resume the simulation. And you can do that. Unlike in the real world, by going ahead and testing your security policies and your procedures in the real life You can see if these things actually work or not and then you try to go hmm, so your lessons learned should basically be based upon what you found out either because Your paper didn't match reality or following the processes or the procedures didn't work or people just didn't know them at which point Maybe you put people on a learning program but they also give you a chance to do things like practice your incident response plan and You can rehearse and revise your existing plans And if you get new employees who come in or some key people come in roles What a great way to showcase how your team works and get a new CIO Hey, we're inviting you to a tabletop exercise that we're doing.

There's a role for the CIO because there's some executive decisions to make. [00:17:00] I run these with up to and including the CEO, which is great because we put roles for that. Now, Steven Jensen is a Senior Director of Operations at Center for Internet Security. He wrote that tabletop exercises are done well.

Quote, allow for the discovery of ways to reduce your threat surface. That's pretty good. And he said, when you rehearse in tabletop format, your written policies go from just being plain policies to becoming well written policies and procedures. Now he gave a talk at a CSO summit where he talked about executing a tabletop exercise, how it helps you identify gaps in your processes and procedures and things such as that.

And in that, and we got the reference in our show notes, he offered eight steps for effective tabletop exercise. And I want to share them with you. Number one. Set your objective. Develop an objective statement. Whether your exercise goals have a framework for your scenarios, and then have some criteria by which you're going to evaluate the success or the lack of success of [00:18:00] your exercise.

So for example, an example objective statement might be, we'll evaluate the incident response plan ransomware demand is received. Make it specific. Let people know who's going to be participating, what it's about. Let people prepare in advance. It's not a pop quiz. And so it's all right for people to know what the subject is, and then it gives them a chance to look up the policies and procedures.

Remember, it's not to try to stump the chump. The goal is to get people to know their stuff, and if they know their stuff in preparation for this tabletop exercise, then they'll know it in the event of a real world emergency, because otherwise, let's face it, policies and procedures and everything else, kind of boring to read.

Hard to write, too. I've written plenty of them in my time, but the whole idea is, is you want other people to be familiar with them. And even if they don't memorize them, they said, Hey, I remember seeing that in such and such a document. They know where to go get it. And then you want to look at what you do in your procedures.

And let's say in the event of this ransomware, the second tip is establish who [00:19:00] is participating. Who is your intended audience? Is it a large scale tabletop where we have C level executives? Do we have other departments in there? Or are we just looking at our IT security team? Or the ops team or something like that.

You want to control the exercise and target it for your intended audience. So you don't have decisions that need to be made that are outside the scope of the people who are there, unless you have something built into your scenario. That says, for example, the CEO is on a plane and. Unable to reach the CEO, and now we have to go ahead and make decisions in that person's absence.

Okay, fine. The third tip, develop your scenarios. Come up with discussion questions. It's like a role playing game. You're going to ask leading questions, but they should be open ended. Meaning, what are you going to do? Rather, are

you going to do this? Yes or no? And therefore, what you want to do is build a conversation.

One of the things that I noted that the senior CISO said, What our leader from a client did yesterday is she said that this was great. We had a lot of communication, a lot of [00:20:00] collaboration. She really appreciated the fact that this tabletop exercise got her staff talking about things and discussing stuff and figuring things out.

Now, in a situation like a ransomware, if you've got senior leadership, you might want to be able to bring up the tough questions such as. Well, what if the files are not recoverable from backups? Do you pay the ransom? Whom do you involve? Do you call law enforcement? Do you call your legal department? Do you call the banker?

Yes. Do you go ahead and try to buy Bitcoin? Whatever it happens to be. Number four, don't skimp on the scheduling. You have to have enough time to complete the event. So you also want to give enough lead time so people can deconflict their calendars. With the key participants, because one or two key people drop out, you don't have an effective tabletop exercise.

So this has to be something that gets locked down into the schedule. If you've got senior leadership backing you up on this, you've got a little bit more ammunition. When someone says, man, I'm kind of busy. I was gonna go fishing that day. Sorry, CEO says you need to be there. [00:21:00] And enough heads up. Now, how long can you do an exercise?

It can go anywhere from one to eight hours. Yesterday, we budgeted one. Guess what? It ran over. I knew it was going to run over, but we had lunch waiting, so it worked. And we were able to reward people. They didn't mind going over, but they seemed to be enjoying it. Realistically, two hours is probably a minimum scenario time for a controlled set of scenarios.

Now, if you go to eight hours, which is a full day, you're going to exhaust and fatigue your participants. And they're going to have 150 to 500 more emails waiting for them when they get out of there. So Only take the time you need to work through your scenario. Don't go high order and lose vision or the sight of the fact that these people have real world jobs to do.

You're taking them out of the real world, but then you want them to re enter the real world with some specialized knowledge and skills and awareness of what came out of your tabletop. Tip number five, set ground rules. Describe the

purpose up front [00:22:00] of the exercise. How is it going to move forward? And roles and responsibilities.

I'm the facilitator. This is the evaluator. This is the scribe. This is the person. This is the observer. They'll be watching. observers will be watching but not participating. And then here are our questions and we allow it to unfold. At the end, you want to do what we call a hot wash or hot wash up.

It's basically, you've finished the tabletop, you got through the last scenario, you've answered all the questions, you've hopefully met your objectives. Now, the idea of a hot wash, you just sit down and write, well, while it's still in your mind, what went well? What did you like? What didn't you like? What did you think was a new thing that we did that we hadn't done before?

What can you gain out of it? This awareness of what you need to do is going to decay rapidly. And as a result, if you wait a day or two, 80 percent of the data is gone. Get it right then and there, before they leave the room. And also capture what didn't go well. And don't just focus on the [00:23:00] content of the exercise, also focus on the format.

It was really cold in here, or we were hungry, or there weren't enough bathroom breaks, or whatever it happens to be. Take that input, don't criticize it, just think about that and how do we work it into the next exercise. And of course, give people an opportunity to suggest improvements. And as a result, what you're going to do is the next time it's going to be better and you're going to get it to the point where people are going to want to go to your table of exercise because it's pretty cool and it's fun and we've got cookies.

Number seven, after you've gone ahead and collected that hot wash, you want to create an AAR. An After Action Report. That's going to be more of a formal type of a document. It might take a week or two before you condense it. You write up the lessons learned, you cross reference things, you say, okay, fine, these are the proposed changes to our policy or our procedures or our processes based upon what we did there.

And then we can write them out and [00:24:00] come up with an action plan. Who fixes this? When's it going to be done? Here's a little Gantt chart, etc. And it actually becomes something real. And then that's the last or the eighth tip is to create an implementation plan. We want to make sure that we go ahead and we introduce new solutions and maybe evaluate them.

Now there is a CIS tabletop exercise guide, which is about 40 pages. It's in the references and it's going to give you some examples. So here's a slightly modified example of one, that was in the CIS exercise guide. Bill, who's your network administrator. He's overworked and underpaid. His bags are packed.

He's ready for a family vacation to Disneyland. When he's tasked with deploying a critical patch, well, in order to make his flight, Bill quickly builds an installation file for the patch. Here's the MSI, boom, deploy it. And then off he goes. Sally, who's the on call desk service technician, starts to begin receiving calls.

Nobody [00:25:00] can log in. Turns out that there was no testing done before that recently installed critical patch was pushed out. Okay. Make your scenario. What do you do? Well, you have to, first of all, have targeted questions. Once you've laid out the scenario, maybe the first question is, what should Sally's response be in the scenario?

What does she normally do day to day? Okay, let's walk it through. We're kind of deciding what that person would do. And then, do any of your on call technicians have the correct expertise to handle the incident? Does somebody else have a global administrator? Can they roll that back? Do they have to call to another tier for help?

Do you have to call and phone a friend, so to speak, as I like to call it, when we have a company that we use? that has technical expertise, and we have part of a contract, we buy a few hours a month, and when we need them, we call them up, and they got some super smart people, and that's great. Is there a defined escalation process?

Let's take a look at them. Here's another one that they offer in this recommendation. Does your organization have a formal change control policy? Well, of course, if you do, this [00:26:00] shouldn't be a pop quiz, I'm thinking you should have it there, and then let's walk through it in the exercise. See, Bill just did something that was quick and easy for him, but probably not within a change control policy.

So, if we have one, great, but then, when was the last time your employees were trained on that? And do we have, well, let's face it, disciplinary procedures or consequences for people when they fail to follow the established procedures? And, in this type of a scenario, can you roll back patches in the event of an unanticipated negative type of an event?

So you'll test your documented policies and procedures, but what will happen sometimes is people will innovate. They come up with ideas. Well, how about we do this? And you go, well, I never thought of that, but that's great. Okay, we're going to do that, and we write that down, and then that's going to potentially work its way into the next set of policies and procedures.

Maybe now is the time to look at automated patching. Instead of having people manually writing scripts [00:27:00] and pushing them out. Is that something you want to put on your road map over the next year or so? To go ahead and budget for and evaluate? Then that goes into your after action report. Real world changes can occur because of the result of your tabletop.

Now I said earlier about the concept of compliance and SOC 2 and things such as that. And so one of the references that I found was talking about how do you go ahead and when would you do compliance? And this comes from PreParadex. com, and what they offer is a concept as follows. That SOC 2 standards encompass nine principles related to incident response planning, and they suggest that tabletop exercises provide a hands on way to validate and improve Those principles.

For example, number one, security policies and procedures. Tabletop exercises ensure security policies are well defined, followed, and regularly updated. I'm quoting from them here, this is not my stuff, but it's good. Number two, incident identification and classification. These exercises help in practicing the identification, classification, and assessment [00:28:00] of incidents.

Good thing for SOC 2. Incident response team. If you involve the designated incident response team, the tabletop exercises will confirm the readiness. For Number four, by exercising test communications and escalation lines, you can ensure that your parties are promptly informed. Number five, by testing and monitoring, you ensure that the valid and validate the effectiveness of your incident response plan.

Number six, your simulated scenarios will encourage a post mortem analysis to learn from successes and failure. So this post incident analysis really helps you improve. Number seven, the exercises ensure that response plans align with your legal and regulatory requirements. Number eight, proper documentation during exercises supports required evidence for SOC 2 compliance.

And number nine, if third parties are involved, exercises would define and test the communication strategies with vendors and third parties. Now, there is an executive incident response guide that you can get from CISA. [00:29:00] And

they also have a CISA tabletop exercise package in their exercise planner handbook.

Now, I'll refer to them. I'm not going to go ahead and try to give you all 50 pages of it. That would be pretty, or 40 pages. That's a lot. But let me give you an outline for the one section where they have the 12 key steps to a successful exercise. Step one, review the documents. You want to know what you're talking about.

Number two, identify the exercise planning team. Now in a smaller organization, it might be me, myself, and I, but in a larger team, you might work. So when I've done tabletop exercises, I'd get the IT security team involved, work with the CISO, part of the CISO's team, and we would develop scenarios so that we would make sure that things work out.

We'd hold a concept and objectives meeting, which is what we did to figure out What is it that we want to do? What's the general concept? Are we going to focus on a breach, focus on ransomware? Are we going to focus on some sort of disaster, etc.? Then hold our initial planning meeting and develop the exercise.

[00:30:00] Once you've done that, we're going to go ahead and hold a midterm planning meeting to say, refining it, re refining it. But remember, you've got some lead time here. And therefore, about the time that you're starting to come together, you might be at the 80 percent level, send out the invitation. It's going to be several weeks in advance, you're not going to surprise anybody, but you continue to exercise development.

Get a final planning meeting and then create and print out your documents. Now, what's interesting is in the scenario development, I work with one client where I was trying to dream up a scenario. They, they had chosen ransomware and we had some extensive conversations about what is their environment look like?

What is their server? What's their operations? What is it, et cetera, their applications. So that the scenario would be realistic. In this particular case, their audience was, from the CEO on down. So you have the technical team responding and then management in different roles. So I thought about it a little bit and I came up with some ideas.

And I remember writing up a scenario. And then we got the next planning call. I got in there and [00:31:00] I explained my scenario. And there's a long silence. Anybody there? Are you still there? Oh, yeah. What's wrong? Someone paused

again. Someone said, that would work. that would take us down. Oh, okay. Well, you don't want to throw that scenario away.

But you say, can you fix that? Okay. And you go, well, yeah, why don't you fix that? We'll use this scenario. So when the CEO turns over and says, could this happen here? You could say, well, it could have except because of this planning, it doesn't. And so that was one of those aha moments where you go, oh yeah, this was supposed to be a simulation.

And for whatever reason, this guy came up with an attack that would work. Some things like that do potentially occur and that's okay because now the whole purpose is to improve things and we really got a fix in there because we shut off that entire lane of attack from some bad guy who'd come up with the same idea that I came up with.

Hold your final planning meetings and print out your documents. When I had mine, we have [00:32:00] documents in front of people. And paper. They can also use the laptops if they want, but you don't want them surfing and watching cat videos, so it's better off to have paper. And then conduct the exercise. This is where the rubber meets the road.

Then after that, you do your hot wash up, draft your after action report, have an improvement plan, have a meeting where you discuss the AAR reports, and then you come out with a finalized plan for what to do. And so those become your cyber security tabletop exercise tips from CISA.

Okay, so that covered an awful lot of ground on tabletop exercises, but I think there's a lot there for you. So again, the reason we do tabletop exercises is not to play gotcha, but to be able to provide a training environment for your people to deal with Real world scenarios or simulated scenarios that look pretty close to reality and then to go ahead and improve ultimately your real world type of a program.

So I'll give you a quick summary. For example, the one I did yesterday I had an agenda, [00:33:00] a tabletop overview, expected outcomes, Introducing the facilitator, which was me because not everybody knew who I was, the actual tabletop itself Which is a big deal and then do the AAR, the after action report. What happened?

And then our takeaways and next steps. And then what I do is I talk about how to structure the exercise. It's made up of multiple rounds. It's a continuously developing story. We tell people to work with the information you're given,

avoid assumptions and don't pretend to be somebody you're not. Don't go outside of the scope of this exercise, phone a friend and ask somebody, whatever, stay within there.

But I also point out that it's okay to be confused. I'll then talk about expected outcomes on the next slide, understanding the challenges that our leadership team might face during a physical attack or cyber attack, figure out our gaps and our readiness, take actions, where the escalation thresholds beyond which this is bigger than something I can handle and I got to kick it up to the next level, and then simulate those communications channels to know who you're going to call, how do you know that person, do you have that person's speed dial and their [00:34:00] phone number.

Oh, it's, it's on SharePoint. Yeah. But SharePoint went down. How do you get to it? okay. I know I have printed out next to my desk on a piece of paper, the phone numbers and emails and the contacts for all of our vendors in case they need to get in touch. Make sure you understand the relationships you need and then get people to work as a team in a crisis.

And so what you want to do is create a baseline scenario. It could be the launch of a new product, it could be the event of a convention, it could be adoption of a new procedure, or it could be something like a ransomware that takes place, and then what you'll do is you'll set up a scenario. Here's your baseline.

This is what's going on. Here's the background. You fill it in. Skies are blue, birds are chirping. Eh, you might not need that much detail. And lay all this out so there's essentially enough format. Throw some information in there. For example, you might have received a contact report from the FBI suggesting there might be some concern with a nation state actor who could be interested in such and such.

We [00:35:00] received reports that such, you know, put a little bit of these ideas in their head at the very beginning. And then what you'll do is you'll have the first scenario around one. Give it a time, give it a date, and say, Here's what's happening. We're going along and then all of a sudden this thing starts to malfunction a little bit.

It looks like it's not working correct. And then, don't just focus on one little thing. Keep a bigger scenario going because you want to develop your scenario into other things. in this particular case, you want to say, hey, this isn't running right. There's other people there. The one I did yesterday was for an exhibition, an event, so the registration system, it's starting to malfunction a little bit.

The queues are getting longer, but we're doing okay on that. The staff reports that things are going slow. So then you have some questions. What do we do if the people come up and they don't have the right ID? That's not a cyber question, but it's an operational idea. Do we badge them or not? What if you have things that arrive to be part of your event, but you're [00:36:00] not sure that they've been properly inspected, or there's a consideration that might have been tampered with?

What are we concerned about? How about the law enforcement alert? Because maybe we had an FBI alert in the first baseline. Do we really take that seriously? Is there somebody coming in? And things that I put in there is, do you bring in external resources to assist? Who are they? How do we pay for them? Are we prepared to negotiate a contract on short notice?

Hmm. Some things you might not think of otherwise. And then summarize questions like, What should we be thinking about right now? And are we starting to see who is making decisions? And is the right person making the decisions? And then on the next prompt, the next round, I said, okay, fine. Now we've got things going.

And then all of a sudden you realize it's something strange is happening. Somebody has done such an event and you're like, Hmm, yeah, there's somebody with a backpack and they're over there by the display and they're kind of large backpack and it's certainly not a laptop backpack. And what do you do about it?

Well, that's not a cybersecurity. It's a physical security, but I included that. [00:37:00] Do you approach them? Do you have security approach them? Do you call 911? how do you go about it? Do you evacuate everybody or just, maybe it's just somebody who likes to carry around a lot of gear? And how do you communicate with people without panicking them?

And then do you have enough information? What other information would you need? And then you ask questions such as, at the end, did anybody in this discussion recommend, for example, calling local law enforcement? And your groups could either be doing it all at once or you can split it out into different teams.

depending upon how large your audience is and their different roles. My third scenario, I had to throw in a cyber attack. So all of a sudden things crash. They don't work anymore. You can't communicate. You can't get your information,

can't get things going, et cetera. Now, what you want to find out is what do we do?

How do you handle that? And in our exercise yesterday, we came up with a whole bunch of. Well, we can't handle that. I said, well, what if we talked about things? And what if you did this, this, and this? Well, that would work. Now it's a 2 percent probability, maybe that this bad thing would [00:38:00] happen, but that's whole idea that we're looking at.

We've already thought about the other 98%. And so what we did is we built a basic procedure for how to go ahead and compensate, compensating controls in the event that things went sideways. And as a result, we were able to go ahead and come up with some action plan. So let's go test this and make sure that it works correctly.

Okay. And then how are we going to do that? Then we had another, event and then we, I threw some scenario and they're like, things are getting really weird. And then people get my cell phones out there. Do you call the cops? You call the fire department, you call for help or whatever. And then it goes viral.

And then the marketing, you got to deal with the fact that people are telephoning and you got to deal with press releases and what came out of that one is, yeah, we need to inform. The staff that nobody talks to the press. It all goes through this one person who is the point of contact for press. Why is that important?

Because people love to talk. And if you've ever read anything, I've heard some of my episodes, I'll quote some of the things from. Example, people like [00:39:00] General George Patton, who said the first report is always wrong. It usually is, because somebody has to provide a report. They don't have all the data, but they don't want to sound like an idiot.

So they fill in the details. Hi, we're live on the scene. There seems to be a disturbance over here in this particular building. Hey, what's going on out there? Well, we're not certain, so let's wait a couple of days until we read the after action report. We'll go through the police reports. We'll go ahead and look at the summaries.

We'll determine that, and we'll give you a solid report so it's only facts. Thanks. You've still got four minutes and 27 seconds and you're live. Oh, okay. aliens came in here and they send it in through here and enough people make stuff up. Let's face it. We all make stuff up in different things. And now today with a lack

of curated news, the problem is, is that most people's news sources are not very, authoritative.

So that was sort of a high level. I don't wanna give away any details of that particular scenario, but that was the most recent one that I did. And that was top of mind for me. And so therefore you're getting a feel for the types of things you can [00:40:00] do both in the lane cyber security and then bring in a little bit of physical stuff as well.

Again, make sure you've got the right people that are in the room so they could go ahead and do it so you're not asking questions that are out of scope. Because if you have the question about, well, do we pay the ransom on ransomware? Is the CEO here? No. CFO here? No. Legal counsel here? No. Well, then don't ask that question because the people who could answer that question aren't there and you want to put them through scenarios.

So, Tabletop Exercises. I hope you understand the value and importance of that and I want you to start doing them. And if you need help doing a Tabletop Exercise, give us a call here at CISO Tradecraft. We can help you be successful. And what we do for a living is we help other people be successful, not just through a podcast.

Drop us a note on CISO Tradecraft. LinkedIn, or communicate with us on our website, and we'll be very pleased to go ahead and give you some guidance or help out or even help run a tabletop exercise for you. We do a lot of other things as well in terms of things such as career advice, as well as helping you with different ideas and [00:41:00] strategies and policies.

We're here to help you become successful in your cybersecurity career journey, and we'd love to be a part of it. So thank you very much for listening to CISO Tradecraft. We appreciate your time and interest and attention and let other people know. Where you get your information so we can have more followers, so we can improve the cybersecurity ecosystem and help more people protect their infrastructure, protect their organizations, and therefore protect you in the long run.

This is your host, G Mark Hardy. Thank you very much for listening. I appreciate your time and attention. And until next time, stay safe out there.